Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	[REDACTED]
THE BUYER:	**The Secretary of State for Justice on behalf of HM Courts and Tribunal Service**
BUYER ADDRESS	**102 Petty France, London, SW1H 9AJ**
THE SUPPLIER:	**Methods Business and Digital Technology Limited**
SUPPLIER ADDRESS:	Saffron House, 6-10 Kirby Street, London, Greater London, EC1N 8TS
REGISTRATION NUMBER:	02485577
DUNS NUMBER:	505275578
SID4GOV ID:	[REDACTED]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 11 December 2024
It's issued under the Framework Contract with the reference number RM6194 for the provision of Back Office Software.

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6194
3. The following Schedules in equal order of precedence:

    - Joint Schedules for **RM6194**
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 7 (Financial Difficulties)
        - Joint Schedule 10 (Rectification Plan)

    - Joint Schedule 11 (Processing Data)
    - Joint Schedule 12 (Supply Chain Visibility)
- Call-Off Schedules for **RM6194**
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 2 (Staff Transfer)
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 7 (Key Supplier Staff)
    - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
    - Call-Off Schedule 9 (Security) Part B
    - Call-Off Schedule 10 (Exit Management)
    - Call-Off Schedule 13 (Implementation Plan and Testing)
    - Call-Off Schedule 14 (Service Levels)
    - Call-Off Schedule 15 (Call-Off Contract Management)
    - Call-Off Schedule 16 (Benchmarking)
    - Call-Off Schedule 18 (Background Checks)
    - Call-Off Schedule 20 (Call-Off Specification)
    - Call-Off Schedule 23 (Supplier-Furnished Terms)
4. CCS Core Terms (version 3.0.10)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6194
6. [Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.]

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS
The following Special Terms are incorporated into this Call-Off Contract:

1. Buyer agrees to comply with the Salesforce Licence Terms of Use detailed within Annex A and acknowledges that these terms are enforceable by Salesforce against any User of their licences. Buyer agrees to comply with the Own Master Subscription Agreement available at www.owndata.com/legal/msa.
2. Buyer acknowledges that yearly licence fees are payable to Salesforce in advance and therefore payment terms from Buyer to Supplier for licences are outlined in the payment schedule within Schedule 5 Pricing.

3. Supplier, as reseller of Salesforce licences, accepts responsibility for warranties to Buyer under the Framework, however, with respect to the licences, the warranties given by Supplier are restricted to those given by Salesforce under their standard terms

CALL-OFF START DATE: 12 December 2024

CALL-OFF EXPIRY DATE: 11 December 2028

CALL-OFF INITIAL PERIOD: **[REDACTED]**

CALL-OFF DELIVERABLES
Option B: See details in Call-Off Schedule 20 (Call-Off Specification)

MAXIMUM LIABILITY
[REDACTED]

CALL-OFF CHARGES
Option B: See details in Call-Off Schedule 5 (Pricing Details)

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
[REDACTED]

BUYER'S INVOICE ADDRESS:
[REDACTED]

BUYER'S AUTHORISED REPRESENTATIVE
[REDACTED]

BUYER'S ENVIRONMENTAL POLICY
[REDACTED]

BUYER'S SECURITY POLICY
[REDACTED]

SUPPLIER'S AUTHORISED REPRESENTATIVE
[REDACTED]

SUPPLIER'S CONTRACT MANAGER
[REDACTED]

PROGRESS REPORT FREQUENCY
Monthly: On the first Working Day of each calendar month or a mutually agreed day]

PROGRESS MEETING FREQUENCY DURING IMPLEMENTATION
Meetings to be held daily or as required throughout the implementation period.

PROGRESS MEETING FREQUENCY DURING BAU
Meetings to be held on a monthly basis, date to be agreed between HMCTS and Methods.

KEY STAFF
[REDACTED]

KEY SUBCONTRACTOR(S)
Not Applicable (registered name if registered)]

COMMERCIALLY SENSITIVE INFORMATION
We categorise our bid responses, including our rate card, as commercially sensitive.

SERVICE CREDITS
Service Credits will accrue in accordance with Call-Off Schedule 14 (Service Levels).
The Service Credit Cap is: 20% of the annual Service Charge
The Service Period is: One Month
A Critical Service Level Failure is: *Occurs when the performance for 4 or more Critical Service Levels calculated over a Quarterly Service Period fall below their respective Service Level Thresholds in that Quarterly Service Period.*

ADDITIONAL INSURANCES
Details of Additional Insurances required in accordance with Joint Schedule 3 (Insurance Requirements) – **No additional Insurances**

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)]

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	[REDACTED]	Signature:	[REDACTED]
Name:	[REDACTED]	Name:	[REDACTED]
Role:	[REDACTED]	Role:	[REDACTED]
Date:	[REDACTED]	Date:	[REDACTED]

Joint Schedules for RM6194

Joint Schedule 1 (Definitions)

1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;

1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings"** as references to obligations under the Contract;

1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract; and

1.3.12 where the Buyer is a Crown Body it shall be treated as contracting with the Crown as a whole.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

"Achieve"	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone and "**Achieved**", "**Achieving**" and "**Achievement**" shall be construed accordingly;
"Additional Insurances"	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
"Admin Fee"	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees;
"Affected Party"	the party seeking to claim relief in respect of a Force Majeure Event;
"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
"Annex"	extra information which supports a Schedule;
"Application Support"	a wide variety of application services, processes and methodologies for maintaining, enhancing, managing and supporting custom or enterprise applications, packaged software applications, or network-delivered applications.
"Approval"	the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly;
"Audit"	the Relevant Authority's right to: a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant

	Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;
"Auditor"	a) the Buyer's internal and external auditors; b) the Buyer's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office; e) any party formally appointed by the Buyer to carry out audit or similar review functions; and f) successors or assigns of any of the above;
"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Balanced Scorecard"	a tool for Call-Off Contact management activity, through measurement of a Supplier's performance against key performance indicator, which the Buyer and Supplier may agree at the Call-Off Contract Start Date;

"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;
"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
"Call-Off Contract Period"	the Contract Period in respect of the Call-Off Contract;
"Call-Off Expiry Date"	the date of the end of a Call-Off Contract as stated in the Order Form;
"Call-Off Incorporated Terms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
"Call-Off Initial Period"	the Initial Period of a Call-Off Contract specified in the Order Form;
"Call-Off Optional Extension Period"	such period or periods beyond which the Call-Off Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form;
"Call-Off Procedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Procedure and Award Criteria);
"Call-Off Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
"Call-Off Start Date"	the date of start of a Call-Off Contract as stated in the Order Form;
"Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
"Cap"	the maximum amount to be paid by the Buyer under a Time and Materials mechanism for the delivery of an agreed scope;

“Capped Time and Materials”	Time and Materials payable up to a specified Cap for delivery of the agreed scope of Deliverables;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	a change of control within the meaning of Section 450 of the Corporation Tax Act 2010;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
"Commercially Sensitive Information"	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Confidential Information"	means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential;

"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS;
"Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"Contract Period"	the term of either a Framework Contract or Call-Off Contract from the earlier of the: e) applicable Start Date; or f) the Effective Date until the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly;
"Controller"	has the meaning given to it in the GDPR;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;
"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: g) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man Day, of engaging the Supplier Staff, including: i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions; iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer;

	h) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets; i) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and j) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but excluding: k) Overhead; l) financing or similar costs; m) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise; n) taxation; o) fines and penalties; p) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and q) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Data Protection Impact Assessment	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable Law about the Processing of personal data and privacy;
"Data Protection Liability Cap"	the amount specified in the Framework Award Form.

"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "**Deliver**" and "**Delivered**" shall be construed accordingly;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable) for the period specified in the Order Form (for the purposes of this definition the **"Disaster Period**");
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);

"Dispute"	any claim, dispute or difference arises out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as: r) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables s) is required by the Supplier in order to provide the Deliverables; and/or t) has been or shall be generated for the purpose of providing the Deliverables;
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"DPA 2018"	the Data Protection Act 2018;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;
"EIR"	the Environmental Information Regulations 2004;
"Electronic Invoice"	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;

"End Date"	the earlier of: u) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or v) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract;
"Environmental Policy"	to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;
"Estimated Year 1 Charges"	the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form;
"Estimated Yearly Charges"	means for the purposes of calculating each Party's annual liability under clause 11.2 : i) in the first Contract Year, the Estimated Year 1 Charges; or ii) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or iii) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;
"Equality and Human Rights Commission"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise);
"Exit Day"	shall have the meaning in the European Union (Withdrawal) Act 2018;
"Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
"Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
"Fixed Price"	the pricing mechanism whereby the Buyer agrees to pay the Supplier based on a capped price which shall cover all work performed and Deliverables required to be provided by the Supplier Staff and all materials used in the project, no matter how much work us required to complete each identified Deliverable within the agreed scope;

"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from: a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract; b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare; c) acts of a Crown Body, local government or regulatory bodies; d) fire, flood or any disaster; or e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding: i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain; ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and iii) any failure of delay caused by a lack of funds;
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"Framework Award Form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
"Framework Contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;
"Framework Contract Period"	the period from the Framework Start Date until the End Date or earlier termination of the Framework Contract;
"Framework Expiry Date"	the date of the end of the Framework Contract as stated in the Framework Award Form;
"Framework Incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;

"Framework Initial Period"	the initial term of the Framework Contract as specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Initial Period may be extended up to a maximum of the number of years in total specified in the Framework Award Form;
"Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
"Framework Special Terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
"Framework Start Date"	the date of start of the Framework Contract as stated in the Framework Award Form;
"Framework Tender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender Response);
"Further Competition Procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Procedure and Award Criteria);
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"General Anti-Abuse Rule"	f) the legislation in Part 5 of the Finance Act 2013 and; and g) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions;
"General Change in Law"	a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any

	electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: i) are supplied to the Supplier by or on behalf of the Authority; or ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract;
"Government Procurement Card"	the Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;
"ICT Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: h) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; i) details of the cost of implementing the proposed Variation; j) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; k) a timetable for the implementation, together with any proposals for the testing of the Variation; and l) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Incremental Fixed Price"	the pricing mechanism where the overall Statement of Work is based on Capped Time and Materials, but where the prices for individual Deliverables Increments are fixed prior to the work being undertaken. The Charges for the first Deliverable Increment or Deliverables Increments for the Statement of Work will be fixed, but the Charges for subsequent Deliverables Increments will be

	reviewed and refined prior to the execution of each subsequent Deliverables Increment within the same Statement of Work;
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Independent Control"	where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly;
"Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;
"Insolvency Event"	m) in respect of a person: n) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or o) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or p) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or q) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or r) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or s) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or t) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or

	u) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or v) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction;
"Installation Works"	all works which the Supplier is to carry out at the beginning of the Call-Off Contract Period to install the Goods in accordance with the Call-Off Contract;
"Intellectual Property Rights" or "IPR"	w) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information; x) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and y) all other rights having equivalent or similar effect in any country or jurisdiction;
"Invoicing Address"	the address to which the Supplier shall Invoice the Buyer as specified in the Order Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies;
"Joint Controller Agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (*Processing Data*);
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
"Joint Control"	where two or more Controllers agree to jointly determine the purposes and means of Processing Personal Data;
"Key Personnel"	the individuals (if any) identified as such in the Order Form;
"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	any Subcontractor:

	z) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or aa) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or bb) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract, and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"KPI Target"	a key performance indicator target included in the Balanced Scorecard;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly;
"Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
"Man Day"	7.5 Man Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day;
"Man Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks;
"Management Charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
"Management Information" or "MI"	the management information specified in Framework Schedule 5 (Management Charges and Information);

"Marketing Contact"	shall be the person identified in the Framework Award Form;
"MI Default"	means when two (2) MI Reports are not provided in any rolling six (6) month period
"MI Failure"	means when an MI report: cc) contains any material errors or material omissions or a missing mandatory field; or dd) is submitted using an incorrect MI reporting Template; or ee) is not submitted by the reporting date (including where a declaration of no business should have been filed);
"MI Report"	means a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
"MI Reporting Template"	means the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task described in the Implementation Plan;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
"Month"	a calendar month and "**Monthly**" shall be interpreted accordingly;
"National Insurance"	contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992;
"New IPR"	ff) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or gg) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;
"Occasion of Tax Non–Compliance"	where: hh) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a

	Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or ii) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;
"Open Book Data"	complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to: jj) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables; kk) operating expenditure relating to the provision of the Deliverables including an analysis showing: i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables; ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each manpower grade; iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; ll) Overheads; mm) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; nn) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; oo) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier; pp) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and qq) the actual Costs profile for each Service Period;
"Order"	means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;

"Order Form Template"	the template in Framework Schedule 6 (Order Form Template and Call-Off Schedules);
"Other Contracting Authority"	any actual or potential Buyer under the Framework Contract;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the Framework Contract, CCS or the Supplier, and in the in the context of a Call-Off Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits;
"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
"Personal Data"	has the meaning given to it in the GDPR;
"Personal Data Breach"	has the meaning given to it in the GDPR;
"Personnel"	all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies;
"Processing"	has the meaning given to it in the GDPR;
"Processor"	has the meaning given to it in the GDPR;
"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;

“Progress Report Frequency”	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;
“Prohibited Acts”	rr) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; ss) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or tt) committing any offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or uu) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;
“Protective Measures”	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.
“Recall”	a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;
"Recipient Party"	the Party which receives or obtains directly or indirectly Confidential Information;
"Rectification Plan"	the Supplier’s plan (or revised plan) to rectify it’s breach using the template in Joint Schedule 10 (Rectification Plan Template)which shall include:

	vv) full details of the Default that has occurred, including a root cause analysis; ww) the actual or anticipated effect of the Default; and xx) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
"Reimbursable Expenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including: yy) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and zz) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential Information"	aaa) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); bbb) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and information derived from any of the above;
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;

"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;
"Reminder Notice"	a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
“Restricted Staff”	any person employed or engaged by either Party, in the capacity of director or in any research, technical, IT, security, engineering, procurement, financial, legal or managerial role who has been engaged in the provision of the Deliverables or management of the Contract either as principal, agent, employee, independent contractor or in any other form of employment or engagement over the previous 12 months, directly worked with or had any material dealings, but shall not include any person employed or engaged in an administrative, clerical, manual or secretarial capacity;
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
“Schedules"	any attachment to a Framework Contract or Call-Off Contract which contains important information specific to each aspect of buying and selling;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);

"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	means the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Credits) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Order Form;
"Services"	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: ccc) the Deliverables are (or are to be) provided; or ddd) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables;
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Software Support and Maintenance"	Software Support and Maintenance includes any software upgrades, annual updates, patches and fixes needed to improve functionality and keep the software in working order;
"Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;
"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form;

"Standards"	any: eee) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; fff) standards detailed in the specification in Schedule 1 (Specification); ggg) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; hhh) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the date specified in the Order Form;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
"Statement of Works" "(SOW)"	the document which, upon its execution by the Buyer and Supplier, shall become incorporated into their Call-Off Contract and outlines the agreed body of works to be undertaken as part of the Call-Off Contract Deliverables. There may be any number of Statements of Work incorporated into a Call-Off Contract and each Statement of Work may include (but is not limited to) the Statement of Requirements, identified output(s), completion date(s) and charging method(s);
"SOW End Date"	the date up to and including this date when the supply of the Deliverables under the Statement of Work shall cease;
"SOW Start Date"	the date of the start of the Statement of Works as stated in the SOW;
"Standing Instructions"	Standing Instructions are a mechanism that supports the implementation of new policy that is mandated across government as a whole or in certain sectors. It is not possible at the Framework Agreement procurement stage to provide for every instance but examples such as the mandate of technical standards i.e. the use of Greening government ICT strategy; or implementation of standardisation across government.
"Storage Media"	the part of any device that is capable of storing and retrieving data;

"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the Framework Award Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
"Supplier Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Supplier's Confidential Information"	iii) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; jjj) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract; kkk) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;
"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;

"Supplier Marketing Contact"	shall be the person identified in the Framework Award Form;
"Supplier Non-Performance"	where the Supplier has failed to: lll) Achieve a Milestone by its Milestone Date; mmm) provide the Goods and/or Services in accordance with the Service Levels ; and/or nnn) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supply Chain Information Report Template"	the document at Annex 1 of Schedule 12 Supply Chain Visibility;
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;
"Tax"	a) all forms of taxation whether direct or indirect; b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
"Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;

"Test Issue"	any variance or non-conformity of the Deliverables or Deliverables from their requirements as set out in a Call-Off Contract;
"Test Plan"	a plan: ooo) for the Testing of the Deliverables; and ppp) setting out other agreed criteria related to the achievement of Milestones;
"Tests and Testing"	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "**Tested**" shall be construed accordingly;
"Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – (i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and (ii) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
"Variation"	has the meaning given to it in Clause 24 (Changing the contract);
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and

"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form.
"Work Day"	a minimum of 7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
"Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer**]** ("**CCS" "the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature	[REDACTED]
Date	[REDACTED]
Name (in Capitals)	[REDACTED]
Address	[REDACTED]
	[REDACTED]

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature	[REDACTED]
Date	[REDACTED]
Name (in Capitals)	[REDACTED]
Address	[REDACTED]

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

[REDACTED]

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

[REDACTED]

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.

1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.

1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor’s name, registered office and company registration number;

1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm’s-length" terms;

1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;

1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and

1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

(d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 7 (Financial Difficulties)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Annex 2 and
"Financial Distress Event"	2 the occurrence or one or more of the following events: a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract; ii) non-payment by the Monitored Company of any financial indebtedness; iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or

	iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company 3 in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;
"Financial Distress Service Continuity Plan"	4 a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	5 Supplier
"Rating Agencies"	6 the rating agencies listed in Annex 1.

2. When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Schedule shall survive:

2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

3. What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or

such other date as may be requested by CCS. For these purposes the "quick ratio" on any date means:

$$\frac{A + B + C}{D}$$

where:

A	is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];
B	is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
C	is the value at the relevant date of all account receivables of the Monitored]; and
D	is the value at the relevant date of the current liabilities of the Monitored Company].

3.4 The Supplier shall:

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as

the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

4.3 If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

4.4 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.4.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

4.4.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

4.4.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.5 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.64.6.

4.6 CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

5.1.3 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial

Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

6. What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

ANNEX 1: RATING AGENCIES

[REDACTED]

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	**Credit rating (long term)**
Supplier	[D&B Threshold]
Methods Business & Digital Technology Limited	Low Risk

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[**Guidance:** Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	

Supplier [Revised] Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Status of the Controller

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where there other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

2. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

3. The Processor shall notify the Controller with undue delay if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it

is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound,

uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller with undue delay if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Personal Data Breach.

7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

12. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

14. The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Independent Controllers of Personal Data

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

21. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

22. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30

GDPR and shall make the record available to the other Party upon reasonable request.

24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

[REDACTED]

Annex 2 - Joint Controller Agreement – NOT USED

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

1. **Undertakings of both Parties**

1.1 The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

  (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

  (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

  (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

  (i) nature of the data to be protected;

  (i) harm that might result from a Personal Data Breach;

  (iii) state of technological development; and

  (iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3**. Data Protection Breach**

3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Relevant Authority and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the Relevant Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4**. Audit**

4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's

data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost,

full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "**Claim Losses**"):

(a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having

regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Joint Schedule 12 (Supply Chain Visibility)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Contracts Finder"	the Government's publishing portal for public sector procurement opportunities;
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium sized enterprises;
"Supply Chain Information Report Template"	the document at Annex 1 of this Schedule 12; and
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

2. Visibility of Sub-Contract Opportunities in the Supply Chain

2.1 The Supplier shall:

2.1.1 **[REDACTED]**

2.1.2 within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contract Finder with details of the successful Subcontractor;

2.1.3 monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder advertised and awarded in its supply chain during the Contract Period;

2.1.4 provide reports on the information at Paragraph 2.1.3 to the Relevant Authority in the format and frequency as reasonably specified by the Relevant Authority; and

2.1.5 promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

2.2 Each advert referred to at Paragraph 2.1.1 of this Schedule 12 shall provide a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder by the Supplier.

2.3 The obligation on the Supplier set out at Paragraph 2.1 shall only apply in respect of Sub-Contract opportunities arising after the Effective Date.

2.4 Notwithstanding Paragraph 2.1, the Authority may by giving its prior Approval, agree that a Sub-Contract opportunity is not required to be advertised by the Supplier on Contracts Finder.

3. Visibility of Supply Chain Spend

3.1 In addition to any other management information requirements set out in the Contract, the Supplier agrees and acknowledges that it shall, at no charge, provide timely, full, accurate and complete SME management information reports (the "SME Management Information Reports") to the Relevant Authority which incorporates the data described in the Supply Chain Information Report Template which is:

(a) the total contract revenue received directly on the Contract;

(b) the total value of sub-contracted revenues under the Contract (including revenues for non-SMEs/non-VCSEs); and

(c) the total value of sub-contracted revenues to SMEs and VCSEs.

3.2 The SME Management Information Reports shall be provided by the Supplier in the correct format as required by the Supply Chain Information Report Template and any guidance issued by the Relevant Authority from time to time. The Supplier agrees that it shall use the Supply Chain Information Report Template to provide the information detailed at Paragraph 3.1(a) –(c) and acknowledges that the template may be changed from time to time (including the data required and/or format) by

the Relevant Authority issuing a replacement version. The Relevant Authority agrees to give at least thirty (30) days' notice in writing of any such change and shall specify the date from which it must be used.

3.3 The Supplier further agrees and acknowledges that it may not make any amendment to the Supply Chain Information Report Template without the prior Approval of the Authority.

Annex 1

[REDACTED]

Call-Off Schedules for RM6194

Call-Off Schedule 1 (Transparency Reports)

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

[REDACTED]

Call-Off Schedule 2 (Staff Transfer)

1. Definitions

1.1 In this Schedule, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Employee Liability"	**1** all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following: a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;
	b) unfair, wrongful or constructive dismissal compensation;
	c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;
	d) compensation for less favourable treatment of part-time workers or fixed term employees;
	e) outstanding debts and unlawful deduction of wages including any PAYE and National Insurance Contributions in relation to payments made by the Buyer or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Sub-contractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions;
	f) claims whether in tort, contract or statute or otherwise;
	any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;
"Former Supplier"	a supplier supplying the Deliverables to the Buyer before the Relevant Transfer Date that are the same as

	or substantially similar to the Deliverables (or any part of the Deliverables) and shall include any Sub-contractor of such supplier (or any Sub-contractor of any such Sub-contractor);
"Partial Termination"	the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);
"Relevant Transfer"	a transfer of employment to which the Employment Regulations applies;
"Relevant Transfer Date"	in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place, and for the purposes of Part D: Pensions, shall include the Commencement Date, where appropriate;
"Supplier's Final Supplier Personnel List"	a list provided by the Supplier of all Supplier Personnel whose will transfer under the Employment Regulations on the Service Transfer Date;
"Supplier's Provisional Supplier Personnel List"	a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;
"Staffing Information"	in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Laws), but including in an anonymised format: (a) their ages, dates of commencement of employment or engagement, gender and place of work;
	(b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;
	(c) the identity of the employer or relevant contracting Party;
	(d) their relevant contractual notice periods and any other terms relating to termination of

		employment, including redundancy procedures, and redundancy payments;
	(e)	their wages, salaries, bonuses and profit sharing arrangements as applicable;
	(f)	details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;
	(g)	any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);
	(h)	details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;
	(i)	copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and
	(j)	any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;
"Term"	the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract;	
"Transferring Buyer Employees"	those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date;	
"Transferring Former Supplier Employees"	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date.	

2. INTERPRETATION

Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity,

undertaking or warranty, the Supplier shall procure that each of its Sub-contractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Sub-contractor, as the case may be and where the Sub-contractor fails to satisfy any claims under such indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

3. Which parts of this Schedule apply

Only the following parts of this Schedule shall apply to this Call Off Contract:

- Part C (No Staff Transfer On Start Date)

Part A: Staff Transfer at the Start Date N/A

Outsourcing from the Buyer

1. What is a relevant transfer

1.1 The Buyer and the Supplier agree that:

1.1.1 the commencement of the provision of the Services or of each relevant part of the Services will be a Relevant Transfer in relation to the Transferring Buyer Employees; and

1.1.2 as a result of the operation of the Employment Regulations, the contracts of employment between the Buyer and the Transferring Buyer Employees (except in relation to any terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or any Sub-Contractor and each such Transferring Buyer Employee.

1.1.3 The Buyer shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of the Transferring Buyer Employees in respect of the period arising up to (but not including) the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions.

2. Indemnities the Buyer must give

2.1 Subject to Paragraph 2.2, the Buyer shall indemnify the Supplier and any Sub-contractor against any Employee Liabilities arising from or as a result of any act or omission by the indemnifying party in respect of any Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee occurring before the Relevant Transfer Date.

2.2 The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Sub-contractor whether occurring or having its origin before, on or after the Relevant Transfer Date.

2.3 Subject to Paragraphs 2.4 and 2.5, if any employee of the Buyer who is not identified as a Transferring Buyer Employee claims, or it is determined in relation to any employees of the Buyer, that his/her contract of employment has been transferred from the Buyer to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations then -

2.3.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;

2.3.2 the Buyer may offer employment to such person, or take such other steps as it considers appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

2.3.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;

2.3.4 if after the period referred to in Paragraph 2.3.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 2.3.1 to 2.3.4 the Buyer will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in this Paragraph 2.3.

2.4 The indemnity in Paragraph 2.3 shall not apply to any claim:

2.4.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or any Sub-contractor; or

2.4.2 (b) any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure.

2.5 The indemnity in Paragraph 2.3 shall not apply to any termination of employment occurring later than 3 Months from the Relevant Transfer Date.

2.6 If the Supplier and/or any Sub-contractor at any point accept the employment of any person as is described in Paragraph 2.3, such person shall be treated as having transferred to the Supplier and/or any Sub-contractor and the Supplier shall comply with such obligations as may be imposed upon it under applicable Law.

3. Indemnities the Supplier must give and its obligations

3.1 Subject to Paragraph 3.2, the Supplier shall indemnify the Buyer against any Employee Liabilities arising from or as a result of any act or omission by the Supplier or any Sub-contractor in respect of any Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee whether occurring before, on or after the Relevant Transfer Date.

3.2 The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Buyer whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Buyer's failure to comply with its obligations under the Employment Regulations.

3.3 The Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of the Transferring Buyer Employees, from (and including) the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions and any other sums due under Part D: Pensions.

4. Information the Supplier must provide

The Supplier shall promptly provide to the Buyer in writing such information as is necessary to enable the Buyer to carry out its duties under regulation 13 of the Employment Regulations. The Buyer shall promptly provide to the Supplier in writing such information as is necessary to enable the Supplier and any Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.

5. Cabinet Office requirements

5.1 The Parties agree that the Principles of Good Employment Practice issued by the Cabinet Office in December 2010 apply to the treatment by the Supplier of employees whose employment begins after the Relevant Transfer Date, and the Supplier undertakes to treat such employees in accordance with the provisions of the Principles of Good Employment Practice.

5.2 The Supplier shall comply with any requirement notified to it by the Buyer relating to pensions in respect of any Transferring Buyer Employee as set down in (i) the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised 2007; (ii) HM Treasury's guidance "Staff Transfers from Central Government: A Fair Deal for Staff Pensions of 1999; (iii) HM Treasury's guidance "Fair deal for staff pensions: procurement of Bulk Transfer Agreements and Related Issues" of June 2004; and/or (iv) the New Fair Deal.

5.3 Any changes embodied in any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraphs 5.1 or 5.2 shall be agreed in accordance with the Variation Procedure.

6. Pensions

6.1 The Supplier shall comply with:

6.1.1 all statutory pension obligations in respect of all Transferring Buyer Employees; and

6.1.2 the provisions in Part D: Pensions.

Part B: Staff transfer at the Start Date N/A

Transfer from a former Supplier on Re-procurement

1. What is a relevant transfer

1.1 The Buyer and the Supplier agree that:

1.1.1 the commencement of the provision of the Services or of any relevant part of the Services will be a Relevant Transfer in relation to the Transferring Former Supplier Employees; and

1.1.2 as a result of the operation of the Employment Regulations, the contracts of employment between each Former Supplier and the Transferring Former Supplier Employees (except in relation to any terms disapplied through the operation of regulation 10(2) of the Employment Regulations) shall have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or any Sub-contractor and each such Transferring Former Supplier Employee.

1.2 The Buyer shall procure that each Former Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of all the Transferring Former Supplier Employees in respect of the period up to (but not including) the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions.

2. Indemnities given by the Former Supplier

2.1 Subject to Paragraph 2.2, the Buyer shall procure that each Former Supplier shall indemnify the Supplier and any Sub-contractor against any Employee Liabilities arising from or as a result of any act or omission by the Former Supplier in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee arising before the Relevant Transfer Date;

2.2 The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Sub-contractor whether occurring or having its origin before, on or after the Relevant Transfer Date.

2.3 Subject to Paragraphs 2.4 and 2.5, if any employee of a Former Supplier who is not identified as a Transferring Former Supplier Employee and claims, and/or it is determined, in relation to such person that his/her contract of employment has been transferred from a Former Supplier to the Supplier

and/or any Notified Sub-contractor pursuant to the Employment Regulations then:

2.3.1 the Supplier will within 5 Working Days of becoming aware of that fact notify the Buyer and the relevant Former Supplier in writing;

2.3.2 the Former Supplier may offer employment to such person, or take such other steps as it considers appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

2.3.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;

2.3.4 if after the period referred to in Paragraph 2.3.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 2.3.1 to 2.3.4 the Buyer shall procure that the Former Supplier will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Former Supplier's employees referred to in Paragraph 2.3.

2.4 The indemnity in Paragraph 2.3 shall not apply to any claim:

2.4.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees, arising as a result of any alleged act or omission of the Supplier and/or any Sub-contractor; or

2.4.2 that the termination of employment was unfair because the Supplier and/or Sub-contractor neglected to follow a fair dismissal procedure.

2.5 The indemnity in Paragraph 2.3 shall not apply to any termination of employment occurring later than 3 Months from the Relevant Transfer Date.

2.6 If the Supplier and/or any Sub-contractor at any point accept the employment of any person as is described in Paragraph 2.3, such person shall be treated as having transferred to the Supplier and/or any Sub-contractor and the Supplier shall comply with such obligations as may be imposed upon it under applicable Law.

3. Indemnities the Supplier must give and its obligations

3.1 Subject to Paragraph 3.1, the Supplier shall indemnify the Buyer, and the Former Supplier against any Employee Liabilities arising from or as a result of any act or omission by the Supplier or any Sub-contractor in respect of any

Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee whether occurring before, on or after the Relevant Transfer Date.

3.2 The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Former Supplier whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Former Supplier's failure to comply with its obligations under the Employment Regulations.

3.3 The Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of all the Transferring Former Supplier Employees, on and from the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions and all such sums due under Part D: Pensions.

4. Information the Supplier must give

The Supplier shall promptly provide to the Buyer and/or at the Buyer's direction, the Former Supplier, in writing such information as is necessary to enable the Buyer and/or the Former Supplier to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Former Supplier shall promptly provide to the Supplier in writing such information as is necessary to enable the Supplier and any Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.

5. Cabinet Office requirements

5.1 The Supplier shall comply with any requirement notified to it by the Buyer relating to pensions in respect of any Transferring Former Supplier Employee as set down in (i) the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised 2007; (ii) HM Treasury's guidance "Staff Transfers from Central Government: A Fair Deal for Staff Pensions of 1999; (iii) HM Treasury's guidance: "Fair deal for staff pensions: procurement of Bulk Transfer Agreements and Related Issues" of June 2004; and/or (iv) the New Fair Deal.

5.2 Any changes embodied in any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraph 5.1 shall be agreed in accordance with the Change Control Procedure.

6. Limits on the Former Supplier's obligations

Notwithstanding any other provisions of this Part B, where in this Part B the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer's must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

7. Pensions

7.1 The Supplier shall comply with:

7.1.1 all statutory pension obligations in respect of all Transferring Former Supplier Employees; and

7.1.2 the provisions in Part D: Pensions.

Part C: No Staff Transfer on the Start Date

1. What happens if there is a staff transfer

1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.

1.2 Subject to Paragraphs 1.3, 1.4 and 1.5, if any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations then:

1.2.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;

1.2.2 the Buyer may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

1.2.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;

1.2.4 if after the period referred to in Paragraph 1.2.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 1.2.1 to 1.2.4:

(a) the Buyer will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2; and

(b) the Buyer will procure that the Former Supplier indemnifies the Supplier and/or any Sub-contractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2.

1.3 The indemnities in Paragraph 1.2 shall not apply to any claim:

1.3.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or Sub-contractor; or

1.3.2 any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure

1.4 The indemnities in Paragraph 1.2 shall not apply to any termination of employment occurring later than 3 Months from the Commencement Date.

1.5 If the Supplier and/or the Sub-contractor does not comply with Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Sub-contractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Sub-contractor.

2. Limits on the Former Supplier's obligations

Where in this Part C the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

Part D: Pensions

1. Definitions

In this Part D, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions), and shall be deemed to include the definitions set out in the Annexes:

"Actuary"	a Fellow of the Institute and Faculty of Actuaries;
"Admission Agreement"	means either or both of the CSPS Admission Agreement (as defined in Annex D1: CSPS) or the LGPS Admission Agreement) as defined in Annex D3: LGPS), as the context requires;
"Broadly Comparable"	(a) in respect of a pension scheme, a status satisfying the condition that there are no identifiable employees who will suffer material detriment overall in terms of future accrual of pension benefits as assessed in accordance with Annex A of New Fair Deal and demonstrated by the issue by the Government Actuary's Department of a broad comparability certificate; and
	(b) in respect of benefits provided for or in respect of a member under a pension scheme, benefits that are consistent with that pension scheme's certificate of broad comparability issued by the Government Actuary's Department, and "**Broad Comparability**" shall be construed accordingly;
"CSPS"	the schemes as defined in Annex D1 to this Part D;
"Fair Deal Employees"	those: (a) Transferring Buyer Employees; and/or
	(b) Transferring Former Supplier Employees; and/or
	(c) employees who are not Transferring Buyer Employees or Transferring Former Supplier Employees but to whom the Employment Regulations apply on the Relevant Transfer Date to transfer their employment to the Supplier or a Sub-contractor, and whose employment is not terminated in accordance with the provisions of Paragraphs 2.3.4 of Parts A or B or Paragraph 1.2.4 of Part C;

	(d) where the Former Supplier becomes the Supplier those employees;
	who at the Commencement Date or Relevant Transfer Date (as appropriate) are or become entitled to New Fair Deal protection in respect of any of the Statutory Schemes as notified by the Buyer;
"Fair Deal Schemes"	means the relevant Statutory Scheme or a Broadly Comparable pension scheme;
"Fund Actuary"	means Fund Actuary as defined in Annex D3 to this Part D;
"LGPS"	the schemes as defined in Annex D3 to this Part D;
"NHSPS"	the schemes as defined in Annex D2 to this Part D;
"New Fair Deal"	the revised Fair Deal position set out in the HM Treasury guidance: "*Fair Deal for Staff Pensions: Staff Transfer from Central Government*" issued in October 2013 including: (a) any amendments to that document immediately prior to the Relevant Transfer Date; and
	(b) any similar pension protection in accordance with the subsequent Annex D1-D3 inclusive as notified to the Supplier by the CCS or Buyer; and
"Statutory Schemes"	means the CSPS, NHSPS or LGPS.

2. Supplier obligations to participate in the pension schemes

2.1 In respect of all or any Fair Deal Employees each of Annex D1: CSPS, Annex D2: NHSPS and/or Annex D3: LGPS shall apply, as appropriate.

2.2 The Supplier undertakes to do all such things and execute any documents (including any relevant Admission Agreement and/or Direction Letter, if necessary) as may be required to enable the Supplier to participate in the appropriate Statutory Scheme in respect of the Fair Deal Employees and shall bear its own costs in such regard.

2.3 The Supplier undertakes:

2.3.1 to pay to the Statutory Schemes all such amounts as are due under the relevant Admission Agreement and/or Direction Letter or otherwise and shall deduct and pay to the Statutory Schemes such employee contributions as are required; and

2.3.2 to be fully responsible for all other costs, contributions, payments and other amounts relating to its participation in the Statutory Schemes, including for the avoidance of doubt any exit payments and the costs of providing any bond, indemnity or guarantee required in relation to such participation.

3. Supplier obligation to provide information

3.1 The Supplier undertakes to the Buyer*:*

3.1.1 to provide all information which the Buyer may reasonably request concerning matters referred to in this Part D as expeditiously as possible; and

3.1.2 not to issue any announcements to any Fair Deal Employee prior to the Relevant Transfer Date concerning the matters stated in this Part D without the consent in writing of the Buyer (such consent not to be unreasonably withheld or delayed).

4. Indemnities the Supplier must give

4.1 The Supplier undertakes to the Buyer to indemnify and keep indemnified CCS, NHS Pensions the Buyer and/or any Replacement Supplier and/or any Replacement Sub-contractor on demand from and against all and any Losses whatsoever arising out of or in connection with any liability towards all and any Fair Deal Employees arising in respect of service on or after the Relevant Transfer Date which arise from any breach by the Supplier of this Part D, and/or the CSPS Admission Agreement and/or the Direction Letter and/or the LGPS Admission Agreement or relates to the payment of benefits under and/or participation in an occupational pension scheme (within the meaning provided for in section 1 of the Pension Schemes Act 1993) or the Fair Deal Schemes.

4.2 The Supplier hereby indemnifies the CCS, NHS Pensions, the Buyer and/or any Replacement Supplier and/or Replacement Sub-contractor from and against all Losses suffered or incurred by it or them which arise from claims by Fair Deal Employees of the Supplier and/or of any Sub-contractor or by any trade unions, elected employee representatives or staff associations in respect of all or any such Fair Deal Employees which Losses:

4.2.1 relate to pension rights in respect of periods of employment on and after the Relevant Transfer Date until the date of termination or expiry of this Contract; or

4.2.2 arise out of the failure of the Supplier and/or any relevant Sub-contractor to comply with the provisions of this Part D before the date of termination or expiry of this Contract.

4.3 The indemnities in this Part D and its Annexes:

4.3.1 shall survive termination of this Contract; and

4.3.2 shall not be affected by the caps on liability contained in Clause 11 (How much you can be held responsible for).

5. What happens if there is a dispute

5.1 The Dispute Resolution Procedure will not apply to this Part D and any dispute between the CCS and/or the Buyer and/or the Supplier or between their respective actuaries or the Fund Actuary about any of the actuarial matters referred to in this Part D and its Annexes shall in the absence of agreement between the CCS and/or the Buyer and/or the Supplier be referred to an independent Actuary:

5.1.1 who will act as an expert and not as an arbitrator;

5.1.2 whose decision will be final and binding on the CCS and/or the Buyer and/or the Supplier; and

5.1.3 whose expenses shall be borne equally by the CCS and/or the Buyer and/or the Supplier unless the independent Actuary shall otherwise direct.

6. Other people's rights

6.1 The Parties agree Clause 19 (Other people's rights in this contract) does not apply and that the CRTPA applies to this Part D to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to him or her or it by the Supplier under this Part D, in his or her or its own right under section 1(1) of the CRTPA.

6.2 Further, the Supplier must ensure that the CRTPA will apply to any Sub-Contract to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to them by the Sub-contractor in his or her or its own right under section 1(1) of the CRTPA.

7. What happens if there is a breach of this Part D

7.1 The Supplier agrees to notify the Buyer should it breach any obligations it has under this Part D and agrees that the Buyer shall be entitled to terminate its Contract for material Default in the event that the Supplier:

7.1.1 commits an irremediable breach of any provision or obligation it has under this Part D; or

7.1.2 commits a breach of any provision or obligation it has under this Part D which, where capable of remedy, it fails to remedy within a reasonable time and in any event within 28 days of the date of a notice from the Buyer giving particulars of the breach and requiring the Supplier to remedy it.

8. Transferring New Fair Deal Employees

8.1 Save on expiry or termination of this Contract, if the employment of any Fair Deal Employee transfers to another employer (by way of a transfer under the Employment Regulations) the Supplier shall and shall procure that any relevant Sub-Contractor shall:

8.1.1 consult with and inform those Fair Deal Employees of the pension provisions relating to that transfer; and

8.1.2 procure that the employer to which the Fair Deal Employees are transferred (the **"New Employer"**) complies with the provisions of this Part D and its Annexes provided that references to the "Supplier" will become references to the New Employer, references to "Relevant Transfer Date" will become references to the date of the transfer to the New Employer and references to "Fair Deal Employees" will become references to the Fair Deal Employees so transferred to the New Employer.

9. What happens to pensions if this Contract ends

The provisions of Part E: Staff Transfer On Exit (Mandatory) apply in relation to pension issues on expiry or termination of this Contract.

10. Broadly Comparable Pension Schemes

10.1 If either:

10.1.1 the terms of any of Paragraphs 2.2 of Annex D1: CSPS, 5.2 of Annex D2: NHSPS and or 4 of Annex D3: LGPS apply; and/or

10.1.2 the Buyer agrees, having considered the exceptional cases provided for in New Fair Deal, (such agreement not to be unreasonably withheld) that the Supplier (and/or its Sub-contractors, if any) need not continue to provide the Fair Deal Employees, who continue to qualify for Fair Deal Protection, with access to the appropriate Statutory Scheme;

the Supplier must (and must, where relevant, procure that each of its Sub-contractors will) ensure that, with effect from the Relevant Transfer Date or if later cessation of participation in the Statutory Scheme until the day before the Service Transfer Date, the relevant Fair Deal Employees will be eligible for membership of a pension scheme under which the benefits are Broadly Comparable to those provided under the relevant Statutory Scheme, and then on such terms as may be decided by the Buyer.

10.2 Where the Supplier has set up a Broadly Comparable pension scheme or schemes pursuant to the provisions of Paragraph 10.1, the Supplier shall (and shall procure that any of its Sub-contractors shall):

10.2.1 supply to the Buyer details of its (or its Sub-contractor's) Broadly Comparable pension scheme and provide a full copy of the valid certificate of broad comparability covering all relevant Fair Deal Employees, as soon as it is able to do so and in any event no later than 28 days before the Relevant Transfer Date;

10.2.2 fully fund any such Broadly Comparable pension scheme in accordance with the funding requirements set by that Broadly Comparable pension scheme's Actuary or by the Government Actuary's Department for the period ending on the Service Transfer Date;

10.2.3 instruct any such Broadly Comparable pension scheme's Actuary to, and to provide all such co-operation and assistance in respect of any such Broadly Comparable pension scheme as

the Replacement Supplier and/or CCS and/or NHS Pension and/or CSPS and/or the relevant Administering Authority and/or the Buyer may reasonably require, to enable the Replacement Supplier to participate in the appropriate Statutory Scheme in respect of any Fair Deal Employee that remain eligible for New Fair Deal protection following a Service Transfer;

10.2.4 provide a replacement Broadly Comparable pension scheme with immediate effect for those Fair Deal Employees who are still employed by the Supplier and/or relevant Sub-contractor and are still eligible for New Fair Deal protection in the event that the Supplier and/or Sub-contractor's Broadly Comparable pension scheme is terminated;

10.2.5 allow and make all necessary arrangements to effect, in respect of any Fair Deal Employee that remains eligible for New Fair Deal protection, following a Service Transfer, the bulk transfer of past service from any such Broadly Comparable pension scheme into the relevant Statutory Scheme and as is relevant on a day for day service basis and to give effect to any transfer of accrued rights required as part of participation under New Fair Deal. For the avoidance of doubt, should the amount offered by the Broadly Comparable pension scheme be less than the amount required by the appropriate Statutory Scheme to fund day for day service (**"Shortfall"**), the Supplier or the Sub-contractor (as agreed between them) must pay the Statutory Scheme, as required, provided that in the absence of any agreement between the Supplier and any Sub-contractor, the Shortfall shall be paid by the Supplier; and

10.2.6 indemnify CCS and/or the Buyer and/or NHS Pension and/or CSPS and/or the relevant Administering Authority and/or on demand for any failure to pay the Shortfall as required under Paragraph 10.2.5 above.

Annex D1:
Civil Service Pensions Schemes (CSPS)

1. Definitions

In this Annex D1: CSPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"CSPS Admission Agreement"	an admission agreement in the form available on the Civil Service Pensions website immediately prior to the Relevant Transfer Date to be entered into for the CSPS in respect of the Services;
"CSPS Eligible Employee"	any Fair Deal Employee who at the relevant time is an eligible employee as defined in the CSPS Admission Agreement;
"CSPS"	the Principal Civil Service Pension Scheme available to Civil Servants and employees of bodies under Schedule 1 of the Superannuation Act 1972 (and eligible employees of other bodies admitted to participate under a determination under section 25 of the Public Service Pensions Act 2013), as governed by rules adopted by Parliament; the Partnership Pension Account and its (i) Ill health Benefits Arrangements and (ii) Death Benefits Arrangements; the Civil Service Additional Voluntary Contribution Scheme; [**Delete** after 30 September 2018: the Designated Stakeholder Pension Scheme which is scheduled to close to new members in September 2018] and "alpha" introduced under The Public Service (Civil Servants and Others) Pensions Regulations 2014.

2. Access to equivalent pension schemes after transfer

2.1 The Supplier shall procure that the Fair Deal Employees, shall be either admitted into, or offered continued membership of, the relevant section of the CSPS that they currently contribute to, or were eligible to join immediately prior to the Relevant Transfer Date or became eligible to join on the Relevant Transfer Date and the Supplier shall procure that the Fair Deal Employees continue to accrue benefits in accordance with the provisions governing the relevant section of the CSPS for service from (and including) the Relevant Transfer Date.

2.2 The Supplier undertakes that should it cease to participate in the CSPS for whatever reason at a time when it has CSPS Eligible Employees, that it will, at no extra cost to the Buyer, provide to any Fair Deal Employee who immediately prior to such cessation of participation remained a CSPS Eligible Employee with access to a pension scheme which is Broadly Comparable to the CSPS on the date the CSPS Eligible Employees ceased to participate in the CSPS.

Annex D2: NHS Pension Schemes

1. Definitions

In this Annex D2: NHSPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Direction Letter"	an NHS Pensions Direction or Determination (as appropriate) issued by the Secretary of State in exercise of the powers conferred by section 7 of the Superannuation (Miscellaneous Provisions) Act 1967 or by section 25 of the Public Service Pensions Act 2013 (as appropriate) and issued to the Supplier or a Sub-contractor of the Supplier (as appropriate) relating to the terms of participation of the Supplier or Sub-contractor in the NHSPS in respect of the NHSPS Eligible Employees;
"NHSPS Eligible Employees"	each of the Fair Deal Employees who at a Relevant Transfer Date was a member of, or was entitled to become a member of, or but for their compulsory transfer of employment would have been entitled to be or become a member of, the NHSPS as a result of either:
	(a) their employment with the Buyer, an NHS Body or other employer which participates automatically in the NHSPS; or
	(b) their employment with a Former Supplier who provides access to the NHSPS pursuant to an NHS Pensions Direction or Determination (as appropriate) issued by the Secretary of State in exercise of the powers conferred by section 7 of the Superannuation (Miscellaneous Provisions) Act 1967 or by section 25 of the Public Service Pensions Act 2013 (as appropriate) in respect of their employment with that Former Supplier (on the basis that they are entitled to protection under New Fair Deal and were permitted to re-join the NHSPS, having been formerly in employment with the Buyer, an NHS Body or other employer who participated automatically in the NHSPS in connection with the Services, prior to being employed by the Former Supplier),
	and, in each case, being continuously engaged for more than fifty per cent (50%) of their employed time in the delivery of services (the same as or similar to the Services).

	For the avoidance of doubt, an individual who is in or entitled to become a member of the NHSPS as a result of being engaged in the Services and being covered by an "open" Direction Letter or other NHSPS "access" facility but who has never been employed directly by an NHS Body (or other body which participates automatically in the NHSPS) is not an NHSPS Eligible Employee;
"NHS Body"	has the meaning given to it in section 275 of the National Health Service Act 2006 as amended by section 138(2)(c) of Schedule 4 to the Health and Social Care Act 2012;
"NHS Pensions"	NHS Pensions as the administrators of the NHSPS or such other body as may from time to time be responsible for relevant administrative functions of the NHSPS;
"NHSPS"	the National Health Service Pension Scheme for England and Wales, established pursuant to the Superannuation Act 1972 and governed by subsequent regulations under that Act including the NHS Pension Scheme Regulations;
"NHS Pension Scheme Arrears"	any failure on the part of the Supplier or its Sub-contractors (if any) to pay employer's contributions or deduct and pay across employee's contributions to the NHSPS or meet any other financial obligations under the NHSPS or any Direction Letter in respect of the NHSPS Eligible Employees;
"NHS Pension Scheme Regulations"	as appropriate, any or all of the National Health Service Pension Scheme Regulations 1995 (SI 1995/300), the National Health Service Pension Scheme Regulations 2008 (SI 2008/653), the National Health Service Pension Scheme Regulations 2015 (2015/94) and any subsequent regulations made in respect of the NHSPS, each as amended from time to time;
"NHS Premature Retirement Rights"	rights to which any Fair Deal Employee (had they remained in the employment of the Buyer, an NHS Body or other employer which participates automatically in the NHSPS) would have been or are entitled under the NHS Pension Scheme Regulations, the NHS Compensation for Premature Retirement Regulations 2002 (SI 2002/1311), the NHS (Injury Benefits) Regulations 1995 (SI 1995/866) and section 45 of the General Whitley Council conditions

	of service, or any other legislative or contractual provision which replaces, amends, extends or consolidates the same from time to time;
"Pension Benefits"	any benefits payable in respect of an individual (including but not limited to pensions related allowances and lump sums) relating to old age, invalidity or survivor's benefits provided under an occupational pension scheme; and
"Retirement Benefits Scheme"	a pension scheme registered under Chapter 2 of Part 4 of the Finance Act 2004.

2. Membership of the NHS Pension Scheme

2.1 In accordance with New Fair Deal, the Supplier and/or any of its Sub-contractors to which the employment of any NHSPS Eligible Employee compulsorily transfers as a result of the award of this Contract, if not an NHS Body or other employer which participates automatically in the NHSPS, must by or as soon as reasonably practicable after the Relevant Transfer Date, each secure a Direction Letter to enable the NHSPS Eligible Employees to retain either continuous active membership of or eligibility for, the NHSPS for so long as they remain employed in connection with the delivery of the Services under this Contract, and have a right to membership or eligibility of that scheme under the terms of the Direction Letter.

2.2 The Supplier must supply to the Buyer by or as soon as reasonably practicable after the Relevant Transfer Date a complete copy of each Direction Letter.

2.3 The Supplier must ensure (and procure that each of its Sub-Contracts (if any) ensures) that all of its NHSPS Eligible Employees have a contractual right to continuous active membership of or eligibility for the NHSPS for so long as they have a right to membership or eligibility of that scheme under the terms of the Direction Letter.

2.4 The Supplier will (and will procure that its Sub-contractors (if any) will) comply with the terms of the Direction Letter, the NHS Pension Scheme Regulations (including any terms which change as a result of changes in Law) and any relevant policy issued by the Department of Health in respect of the NHSPS Eligible Employees for so long as it remains bound by the terms of any such Direction Letter.

2.5 Where any employee omitted from the Direction Letter supplied in accordance with Paragraph 2 of this Annex are subsequently found to be an NHSPS Eligible Employee, the Supplier will (and will procure that its Sub-contractors (if any) will) treat that person as if they had been an NHSPS Eligible Employee from the Relevant Transfer Date so that their Pension Benefits and NHS Premature Retirement Rights are not adversely affected.

2.6 The Supplier will (and will procure that its Sub-contractors (if any) will) as soon as reasonably practicable and at its (or its Sub-contractor's) cost, obtain

any guarantee, bond or indemnity that may from time to time be required by the Secretary of State for Health.

3. Access to NHS Pension Schemes after transfer

The Supplier will procure that with effect from the Relevant Transfer Date the NHSPS Eligible Employees shall be either eligible for or remain in continuous active membership of (as the case may be) the NHSPS for employment from (and including) the Relevant Transfer Date.

4. Continuation of early retirement rights after transfer

From the Relevant Transfer Date until the Service Transfer Date, the Supplier must provide (and/or must ensure that its Sub-contractors (if any) provide) NHS Premature Retirement Rights in respect of the NHSPS Eligible Employees that are identical to the benefits they would have received had they remained employees of the Buyer, an NHS Body or other employer which participates automatically in the NHSPS.

5. What the buyer do if the Supplier breaches its pension obligations

5.1 The Supplier agrees that the Buyer is entitled to make arrangements with NHS Pensions for the Buyer to be notified if the Supplier (or its Sub-contractor) breaches the terms of its Direction Letter. Notwithstanding the provisions of the foregoing, the Supplier shall notify the Buyer in the event that it (or its Sub-contractor) breaches the terms of its Direction Letter.

5.2 If the Buyer is entitled to terminate the Contract or the Supplier (or its Sub-contractor, if relevant) ceases to participate in the NHSPS for whatever other reason, the Buyer may in its sole discretion, and instead of exercising its right to terminate this Contract where relevant, permit the Supplier (or any such Sub-contractor, as appropriate) to offer Broadly Comparable Pension Benefits, on such terms as decided by the Buyer. The provisions of Paragraph 10 (Bulk Transfer Obligations in relation to any Broadly Comparable pension scheme) of Part D: Pensions shall apply in relation to any Broadly Comparable pension scheme established by the Supplier or its Sub-contractors.

5.3 In addition to the Buyer's right to terminate the Contract, if the Buyer is notified by NHS Pensions of any NHS Pension Scheme Arrears, the Buyer will be entitled to deduct all or part of those arrears from any amount due to be paid under this Contract or otherwise.

6. Compensation when pension scheme access can’t be provided

6.1 If the Supplier (or its Sub-contractor, if relevant) is unable to provide the NHSPS Eligible Employees with either:

6.1.1 membership of the NHSPS (having used its best endeavours to secure a Direction Letter); or

6.1.2 access to a Broadly Comparable pension scheme,

the Buyer may in its sole discretion permit the Supplier (or any of its Sub-contractors) to compensate the NHSPS Eligible Employees in a manner that is Broadly Comparable or equivalent in cash terms, the Supplier (or

Sub-contractor as relevant) having consulted with a view to reaching agreement with any recognised trade union or, in the absence of such body, the NHSPS Eligible Employees. The Supplier must meet (or must procure that the relevant Sub-contractor meets) the costs of the Buyer determining whether the level of compensation offered is reasonable in the circumstances.

6.2 This flexibility for the Buyer to allow compensation in place of Pension Benefits is in addition to and not instead of the Buyer's right to terminate the Contract.

7. Indemnities that a Supplier must give

7.1 The Supplier must indemnify and keep indemnified the CCS, the Buyer and any Replacement Supplier against all Losses arising out of any claim by any NHSPS Eligible Employee that the provision of (or failure to provide) Pension Benefits and NHS Premature Retirement Rights from the Relevant Transfer Date, or the level of such benefit provided, constitutes a breach of his or her employment rights.

7.2 The Supplier must indemnify and keep indemnified the Buyer, NHS Pensions and any Replacement Supplier against all Losses arising out of the Supplier (or its Sub-contractor) allowing anyone who is not an NHSPS Eligible Employee to join or claim membership of the NHSPS at any time during the Contract Period.

8. Sub-Contractors

8.1 If the Supplier enters into a Sub-Contract for the delivery of all or part or any component of the Services which will involve the transfer of employment of any NHSPS Eligible Employee it will impose obligations on its Sub-contractor in identical terms as those imposed on the Supplier in relation to Pension Benefits and NHS Premature Retirement Rights by this Annex, including requiring that:

8.1.1 if the Supplier has secured a Direction Letter, the Sub-contractor also secures a Direction Letter in respect of the NHSPS Eligible Employees for their future service with the Sub-contractor as a condition of being awarded the Sub-Contract and the Supplier shall be responsible for ensuring that the Buyer receives a complete copy of each such Sub-contractor direction letter as soon as reasonably practicable; or

8.1.2 if, in accordance with Paragraph 4 of this Annex, the Supplier has offered the NHSPS Eligible Employees access to a pension scheme under which the benefits are Broadly Comparable to those provided under the NHSPS, the Sub-contractor either secures a Direction Letter in respect of the NHSPS Eligible Employees or (with the prior consent of the Buyer) provides NHSPS Eligible Employees with access to a scheme with Pension Benefits which are Broadly Comparable to those provided under the NHSPS whereupon the provisions of Paragraph 10 below (Bulk Transfer Obligations in relation to any Broadly Comparable Scheme) shall apply.

8.2 The Supplier shall procure that each Sub-contractor provides indemnities to the Buyer, NHS Pensions and/or any Replacement Supplier and/or Replacement Sub-contractor that are identical to the indemnities set out in Paragraph 7 of this Annex B. Where a Sub-contractor fails to satisfy any claim made under such one or more indemnities, the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

Annex D3:

Local Government Pension Schemes (LGPS)

1. Definitions

1.1 In this Annex D3: LGPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"**Administering Authority**"	in relation to **the Fund [insert name],** the relevant Administering Authority of that Fund for the purposes of the Local Government Pension Scheme Regulations 2013;
"**Fund Actuary**"	the actuary to a Fund appointed by the Administering Authority of that Fund;
"**Fund**"	**[insert name], a pension fund within the LGPS;**
"**LGPS**"	the Local Government Pension Scheme as governed by the LGPS Regulations, and any other regulations (in each case as amended from time to time) which are from time to time applicable to the Local Government Pension Scheme;
"**LGPS Admission Agreement**"	an admission agreement within the meaning in Schedule 1 of the Local Government Pension Scheme Regulations 2013;
"**LGPS Admission Body**"	an admission body (within the meaning of Part 3 of Schedule 2 of the Local Government Pension Scheme Regulations 2013);
"**LGPS Eligible Employees**"	any Fair Deal Employee who at the relevant time is an eligible employee as defined in the LGPS Admission Agreement or otherwise any Fair Deal Employees who immediately before the Relevant Transfer Date was a member of, or was entitled to become a member of, or but for their compulsory transfer of employment would have been entitled to be or become a member of, the LGPS or of a scheme Broadly Comparable to the LGPS; and
"**LGPS Regulations**"	the Local Government Pension Scheme Regulations 2013 (SI 2013/2356) and The Local Government Pension Scheme (Transitional Provisions, Savings and Amendment) Regulations 2014, and any other regulations (in each case as amended from time to time) which are from time to time applicable to the LGPS.

2. Supplier must become a LGPS admission body

2.1 Where the Supplier employs any LGPS Eligible Employees from a Relevant Transfer Date, the Supplier shall become an LGPS Admission Body and shall on or before the Relevant Transfer Date enter into a LGPS Admission Agreement with the Administering Authority which will have effect from and including the Relevant Transfer Date.

2.2 The LGPS Admission Agreement must ensure that all LGPS Eligible Employees covered by that Agreement who were active LGPS members immediately before the Relevant Transfer Date are admitted to the LGPS with effect on and from the Relevant Transfer Date. Any LGPS Eligible Employees who were eligible to join the LGPS but were not active LGPS members immediately before the Relevant Transfer Date must retain the ability to join the LGPS after the Relevant Transfer Date if they wish to do so.

2.3 The Supplier shall provide any indemnity, bond or guarantee required by an Administering Authority in relation to an LGPS Admission Agreement.

2.4 The Supplier shall not automatically enrol or re-enrol for the purposes of the Pensions Act 2008 any LGPS Eligible Employees in any pension scheme other than the LGPS.

3. Right of set-off

The Buyer shall have a right to set off against any payments due to the Supplier under the Contract an amount equal to any overdue employer and employee contributions and other payments (and interest payable under the LGPS Regulations) due from the Supplier (or from any relevant Sub-contractor) under an LGPS Admission Agreement and shall pay such amount to the relevant Fund.

4. Supplier ceases to be an LGPS Admission Body

If the Supplier employs any LGPS Eligible Employees from a Relevant Transfer Date and the Supplier either cannot or does not participate in the LGPS, the Supplier shall offer such LGPS Eligible Employee membership of a pension scheme Broadly Comparable to the LGPS.

5. Discretionary benefits

Where the Supplier is an LGPS Admission Body, the Supplier shall award benefits to the LGPS Eligible Employees under the LGPS in circumstances where the LGPS Eligible Employees would have received such benefits had they still been employed by their previous employer. Where such benefits are of a discretionary nature, they shall be awarded on the basis of the previous employer's written policy in relation to such benefits at the time of the Relevant Transfer Date.

Annex D4: Other Schemes

[Placeholder for Pension Schemes other than LGPS, CSPS & NHSPS]

Part E: Staff Transfer on Exit

1. Obligations before a Staff Transfer

1.1 The Supplier agrees that within 20 Working Days of the earliest of:

1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;

1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;

1.1.3 the date which is 12 Months before the end of the Term; and

1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

it shall provide in a suitably anonymised format so as to comply with the Data Protection Laws, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Sub-contractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) the Staffing Information in relation to the Supplier's Final Supplier Personnel List (insofar as such information has not previously been provided).

1.3 The Buyer shall be permitted to use and disclose information provided by the Supplier under Paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Sub-contractor.

1.4 The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Sub-contractor that all information provided pursuant to Paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.

1.5 From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall, unless otherwise instructed by the Buyer (acting reasonably):

not replace or re-deploy any Supplier Personnel listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person he/she replaces

not make, promise, propose, permit or implement any material changes to the terms and conditions of (i) employment and/or (ii) pensions, retirement and death benefits (including not to make pensionable any category of earnings which were not previously pensionable or reduce the pension contributions payable) of the Supplier Personnel (including any payments connected with the termination of employment);

1.5.1 not increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;

1.5.2 not introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;

1.5.3 not increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);

1.5.4 not terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;

1.5.5 not dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Buyer and/or the Replacement Supplier and/or Replacement Sub-contractor;

1.5.6 give the Buyer and/or the Replacement Supplier and/or Replacement Sub-contractor reasonable access to Supplier Personnel and/or their consultation representatives to inform them of the intended transfer and consult any measures envisaged by the Buyer, Replacement Supplier and/or Replacement Sub-contractor in respect of persons expected to be Transferring Supplier Employees;

1.5.7 co-operate with the Buyer and the Replacement Supplier to ensure an effective consultation process and smooth transfer in respect of Transferring Supplier Employees in line with good employee relations and the effective continuity of the Services, and to allow for participation in any pension arrangements to be put in place to comply with New Fair Deal;

1.5.8 promptly notify the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Sub-contractor of any notice to terminate employment given by the Supplier or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect;

1.5.9 not for a period of 12 Months from the Service Transfer Date re-employ or re-engage or entice any employees, suppliers or Sub-contractors whose employment or engagement is

transferred to the Buyer and/or the Replacement Supplier (unless otherwise instructed by the Buyer (acting reasonably));

1.5.10 not to adversely affect pension rights accrued by all and any Fair Deal Employees in the period ending on the Service Transfer Date;

1.5.11 fully fund any Broadly Comparable pension schemes set up by the Supplier;

1.5.12 maintain such documents and information as will be reasonably required to manage the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Sub-contractor in the provision of the Services on the expiry or termination of this Contract (including without limitation identification of the Fair Deal Employees);

1.5.13 promptly provide to the Buyer such documents and information mentioned in Paragraph 3.1.1 of Part D: Pensions which the Buyer may reasonably request in advance of the expiry or termination of this Contract; and

1.5.14 fully co-operate (and procure that the trustees of any Broadly Comparable pension scheme shall fully co-operate) with the reasonable requests of the Supplier relating to any administrative tasks necessary to deal with the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Sub-contractor in the provision of the Services on the expiry or termination of this Contract.

1.6 On or around each anniversary of the Effective Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide such information as the Buyer may reasonably require which shall include:

1.6.1 the numbers of employees engaged in providing the Services;

1.6.2 the percentage of time spent by each employee engaged in providing the Services;

1.6.3 the extent to which each employee qualifies for membership of any of the Fair Deal Schemes (as defined in Part D: Pensions); and

1.6.4 a description of the nature of the work undertaken by each employee by location.

1.7 The Supplier shall provide all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Sub-contractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within

5 Working Days following the Service Transfer Date, the Supplier shall provide to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Sub-contractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:

1.7.1 the most recent month's copy pay slip data;

1.7.2 details of cumulative pay for tax and pension purposes;

1.7.3 details of cumulative tax paid;

1.7.4 tax code;

1.7.5 details of any voluntary deductions from pay; and

1.7.6 bank/building society account details for payroll purposes.

2. Staff Transfer when the contract ends

2.1 A change in the identity of the supplier of the Services (or part of the Services), howsoever arising, may constitute a Relevant Transfer to which the Employment Regulations will apply. The Buyer and the Supplier agree that where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Sub-contractor (as the case may be) and each such Transferring Supplier Employee.

2.2 The Supplier shall comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Fair Deal Schemes (as defined in Part D: Pensions).

2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Sub-contractor against any Employee Liabilities arising from or as a result of any act or omission of the Supplier or any Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date.

2.4 The indemnity in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Sub-contractor whether occurring or having its origin before, on or after the Service Transfer Date.

2.5 Subject to Paragraphs 2.6 and 2.7, if any employee of the Supplier who is not identified in the Supplier's Final Transferring Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the

Replacement Supplier and/or Replacement Sub-contractor pursuant to the Employment Regulations then.

2.5.1 the Replacement Supplier and/or Replacement Sub-contractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing;

2.5.2 the Supplier may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Sub-contractor;

2.5.3 if such offer of employment is accepted, the Replacement Supplier and/or Replacement Sub-contractor shall immediately release the person from its employment;

2.5.4 if after the period referred to in Paragraph 2.5.2 no such offer has been made, or such offer has been made but not accepted, the Replacement Supplier and/or Replacement Sub-contractor may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Replacement Supplier's and/or Replacement Sub-contractor's compliance with Paragraphs 2.5.1 to 2.5.4 the Supplier will indemnify the Replacement Supplier and/or Replacement Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees referred to in Paragraph 2.5.

2.6 The indemnity in Paragraph 2.5 shall not apply to:

2.6.1 (a) any claim for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief, or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees, arising as a result of any alleged act or omission of the Replacement Supplier and/or Replacement Sub-contractor, or

2.6.2 (b) any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Sub-contractor neglected to follow a fair dismissal procedure.

2.7 The indemnity in Paragraph 2.5 shall not apply to any termination of employment occurring later than 3 Months from the Service Transfer Date.

2.8 If at any point the Replacement Supplier and/or Replacement Sub-contract accepts the employment of any such person as is described in Paragraph 2.5, such person shall be treated as a Transferring Supplier Employee and Paragraph 2.5 shall cease to apply to such person.

2.9 The Supplier shall promptly provide the Buyer and any Replacement Supplier and/or Replacement Sub-contractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or

Replacement Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Sub-contractor, shall promptly provide to the Supplier and each Sub-contractor in writing such information as is necessary to enable the Supplier and each Sub-contractor to carry out their respective duties under regulation 13 of the Employment Regulations.

2.10 Subject to Paragraph 2.9, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Sub-contractor and its Sub-contractors against any Employee Liabilities arising from or as a result of any act or omission, whether occurring before, on or after the Service Transfer Date, of the Replacement Supplier and/or Replacement Sub-contractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee.

2.11 The indemnity in Paragraph 2.10 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Sub-contractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Sub-contractor (as applicable) to comply with its obligations under the Employment Regulations, or to the extent the Employee Liabilities arise out of the termination of employment of any person who is not identified in the Supplier's Final Supplier Personnel List in accordance with Paragraph 2.5 (and subject to the limitations set out in Paragraphs 2.6 and 2.7 above).

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2. Supplier's Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

- 2.3.1 identifying the emergence of relevant new and evolving technologies;
- 2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);
- 2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and
- 2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 5 (Pricing Details)

[REDACTED]

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Annex 1 to this Schedule lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Annex 1- Key Roles

[REDACTED]

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"BCDR Plan"	1 has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2 has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster Recovery Deliverables"	3 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	4 has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	5 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	6 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	7 has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	8 has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

2.1 The Buyer and the Supplier recognise that, where specified in Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Buyer recognises that in most cases the Supplier will have in place a BCDR Plan for their services which will meet industry standards and satisfy the Buyer's requirements. Where this is the case this should be provided to the Customer at the earliest opportunity. It is acknowledged that as these form part of a standard service it may not be possible for a Customer to request adjustments to the plan.

2.3 At least ninety (90) Working Days after the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

2.3.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

2.3.2 the recovery of the Deliverables in the event of a Disaster

2.4 The BCDR Plan shall be divided into three sections:

2.4.1 Section 1 which shall set out general principles applicable to the BCDR Plan;

2.4.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

2.4.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

2.5 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

3.2.4 it details a process for the management of disaster recovery testing.

3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

4.2 The Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

5.2.3 loss of the Supplier's helpdesk or CAFM system;

5.2.4 loss of a Subcontractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

5.2.13 testing and management arrangements.

6. Review and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

6.1.1 on a regular basis and as a minimum once every six (6) Months;

6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

7.1.1 regularly and in any event not less than once in every Contract Year;

7.1.2 in the event of any major reconfiguration of the Deliverables

7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).

7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

7.5.1 the outcome of the test;

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9. Circumstances beyond your control

9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Sched

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements – NOT USED

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	1 the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"),

	information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 2 in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

2. Complying with security requirements and updates to them

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Buyers Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer

Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 **Development of the Security Management Plan**

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in

accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 **Amendment of the Security Management Plan**

4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

a) suggested improvements to the effectiveness of the Security Management Plan;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Part B: Long Form Security Requirements

1. Definitions

1.1 In this Schedule the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	4 means the occurrence of: a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 5 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	6 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	7 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.4 **[REDACTED]**

2.5 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.6 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.7 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.8 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.9 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.3 at all times provide a level of security which:

a) is in accordance with the Law and this Contract;

b) complies with the Baseline Security Requirements;

c) as a minimum demonstrates Good Industry Practice;

d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy

e) [REDACTED]

f) security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

g) addresses issues of incompatibility with the Supplier's own organisational security policies; and

h) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall

use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:
Baseline security requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

[ ]

Call-Off Schedule 10 (Exit Management)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Exclusive Assets"	1 Supplier Assets used exclusively by the Supplierin the provision of the Deliverables;
"Exit Information"	2 has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	3 the person appointed by each Party to manage their respective obligations under this Schedule;
"Net Book Value"	4 the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	5 those Supplier Assets used by the Supplier in connection with the Deliverables but which are also used by the Supplier for other purposes;
"Registers"	6 the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	7 any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	8 any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	9 the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;

"Termination Assistance Notice"	10 has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	11 the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	12 Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	13 Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	14 has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	15 has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for contract exit

2.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the

Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) every six (6) months throughout the Contract Period; and

(b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the date that the Supplier ceases to provide the Deliverables.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than six (6) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.3 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service

Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 13 (Implementation Plan and Testing)
Part A - Implementation

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Delay"	a) a delay in the Achievement of a Milestone by its Milestone Date; or

	b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	has the meaning given to it in Paragraph 7.1;

2. Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 15 days after the Call-Off Contract Start Date.

2.2 The draft Implementation Plan:

2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and

2.2.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

2.5 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

3. Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

3.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

3.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

4. Security requirements before the Start Date

4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5. What to do if there is a Delay

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

6. Compensation for a Delay

6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;

6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

7. Implementation Plan

7.1 The Implementation Period will be at most, a six (6) Month period.

7.2 During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.

7.3 In accordance with the Implementation Plan, the Supplier shall:

7.3.1 work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;

7.3.2 work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and

7.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.

7.5 In addition, the Supplier shall:

7.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract;

7.5.3 produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

(a) the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

(b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

7.5.4 manage and report progress against the Implementation Plan;

7.5.5 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

7.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

7.5.7 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

Annex 1: Implementation Plan

[REDACTED]

Milestone	Deliverable Items
Project start	Initiation document
Requirements Gathering	Produce draft technical, service and operational process flows
Solution Design Phase Completion	Contribution to HMCTS Solution Design artefacts including; • High Level Design (HLD) • Low Level Design (LLD) • IT Health Check (ITHC) • Data Protection Impact Assessment (DPIA)
Service Design Phase Completion	Create a plan that demonstrates meeting the delivery and support of the Services contractual obligations, including Service Levels and Performance Monitoring requirements as set out in the Call-Off Schedule 14 (Service Levels).
Build and Configuration Phase Completion	Build and configuration of the solution completed in line with specified requirements and approved designs including the technical and service designs.
Data Migration Phase Completion	Data migration plan approved Data migration completed and signed off
Deployment Completion	Deployment Plan agreed Operational Readiness Review completed
Testing Phase Start	Testing strategy (and results sharing) agreed
User Acceptance Testing (UAT)	Test Plan agreed Test Success Criteria for all Tests agreed Test Issue Management Log published
Testing Phase Ends	Test Reports published Cutover Plan agreed
Service Transition	Service Desk in place Service Level reporting in place Knowledge Base in place Agreement to enter Early Life Support (ELS) period
System and Services Go-Live	Agreement to exit ELS by completing the services acceptance process, seeking service readiness from the Buyer, and executing service transfer plans

Part B - Testing

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Component"	any constituent parts of the Deliverables;
"Material Test Issue"	a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Issue Management Log"	a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;
"Test Issue Threshold"	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Reports"	the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule;
"Test Strategy"	a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;
"Test Success Criteria"	in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule;
"Test Witness"	any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and
"Testing Procedures"	the applicable testing procedures and Test Success Criteria set out in this Schedule.

2. How testing should work

2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.

2.2 The Supplier shall not submit any Deliverable for Testing:

2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and

2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

3. Planning for testing

3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.

3.2 The final Test Strategy shall include:

3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;

3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;

3.2.4 the procedure to be followed to sign off each Test;

3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;

3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;

3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;

3.2.8 the technical environments required to support the Tests; and

3.2.9 the procedure for managing the configuration of the Test environments.

4. Preparing for Testing

4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.

4.2 Each Test Plan shall include as a minimum:

4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and

4.2.2 a detailed procedure for the Tests to be carried out.

4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

5. Passing Testing

5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. How Deliverables will be tested

6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

6.2 Each Test Specification shall include as a minimum:

6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4 Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

7. Performing the tests

7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.

7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.

7.4 The Buyer may raise and close Test Issues during the Test witnessing process.

7.5 The Supplier shall provide to the Buyer in relation to each Test:

7.5.1 a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and

7.5.2 the final Test Report within 5 Working Days of completion of Testing.

7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

7.6.1 an overview of the Testing conducted;

7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;

7.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

7.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 8.1; and

7.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

7.7 When the Supplier has completed a Milestone it shall submit any Deliverables relating to that Milestone for Testing.

7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier, any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

8. Discovering Problems

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable

to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

9. Test witnessing

9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10. Auditing the quality of the test

10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.

10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for

the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

11. Outcome of the testing

11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;

11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:

11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.

11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.

11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.

11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer's report pursuant to Paragraph 10.5); and

11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

12. Risk

12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:

12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or

12.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

2.1.1 causes a Component to become unusable;

2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

3.1 This is an error which:

3.1.1 causes a Component to become unusable;

3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

5. Severity 5 Error

5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

Annex 2: Satisfaction Certificate

To: [insert name of Supplier]
From: [insert name of Buyer]
[insert Date dd/mm/yyyy]

Dear Sirs,

Satisfaction Certificate

Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].
We refer to the agreement (**"Call-Off Contract"**) [insert Call-Off Contract reference number] relating to the provision of the [insert description of the Deliverables] between the [*insert Buyer name*] (**"Buyer"**) and [*insert Supplier name*] (**"Supplier"**) dated [*insert Call-Off Start Date dd/mm/yyyy*].
The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully
[insert Name]
[insert Position]
acting on behalf of [insert name of Buyer]

Call-Off Schedule 14 (Service Levels)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

1.2

1.3

[REDACTED]

"Application Managed Service"	The Application Managed Service is the name given to the service offered by the Supplier in Supplier response question 4.12. The service provides for both third-line ITIL standard incident response for

	P1-P3 incidents that impact the Production instance of JFEPS; time to make changes to the JFEPS Salesforce configuration to ensure that JFEPS remains relevant to prevailing business requirements during the term of the contract; and Service Management which coordinates activity with the JFEPS live service management as well as producing agreed monthly reporting and attendance at service review meetings.
"Development Environment"	This development environment is used to create a fix for the incident raised. When completed, the code is deployed to the QA environment
"QA Environment"	The QA environment is used for Unit Test and the Quality Assurance Test of the provided fix. When completed, the code is deployed to the UAT environment.
"UAT Environment"	This is the User Acceptance Test environment the Buyer will use during the project and in-live running. The UAT environment is used twofold. Firstly, the incident raised is recreated in the UAT environment before being passed to the development team as required. Secondly, by the Buyer team to test and validate the fix that has come from the QA environment, prior to the code then being then being deployed at an agreed time to production
"Production Environment"	The Production Environment is the secure live-running environment for the running of JFEPS in live. Incident fixes are deployed to the Production environment once the Buyer has completed UAT and has authorised the deployment into Production environment. A short production test is completed to validate the fix. The incident is closed.
"Service Credit Cap"	20% of the annual Service Charge
"Critical Service Level"	Service Level ID 2-71 inclusive;
"Annual Service Charge"	The Application Managed Service as described in Supplier proposal answer 4.12
"Critical Service Level Failure"	Occurs when the performance for 4 or more Critical Service Levels calculated over a Quarterly Service Period fall below their respective Service Level Thresholds in that Quarterly Service Period; Such Critical Service Level Failures shall be attributable to the Services provided by the Supplier and shall not, for example, relate to third-party systems beyond the Supplier's control that may

	impact the availability of the service. All such Critical Service Level Failures shall be mutually agreed at the monthly service meeting. In addition, Critical Service Level Failures can only apply to incidents within the Monthly Service Hours Cap.
"Core Service Operating Hours"	Defined as 08:00 to 20:00 Monday – Friday (London GMT/BST) Services must be **available** to end users during core service operating hours.
"Monthly Service Hours Cap"	The Supplier includes a fixed cost 40 hours of Applications Managed Service time per month as a time capped service. Additional hours may be purchased upon request. The Supplier will respond to and resolve incidents even if the Cap has been exceeded.
"Maximum Service Credit per Service Level per Service Period"	Means the amount set out against the relevant Service Level;
"Monthly Service Credit Cap"	shall be 20% of the Service Charges for the Service Period;
"Primary Operational Support Service Hours"	Defined as 08:00 to 18:00 Monday – Friday (London GMT/BST). Service must be supported during the Core Service Operating Hours.
"Resolved"	The process of fixing an issue and restoring normal system functionality. The goal is to minimise the impact of an incident on users. Actions taken by the Supplier include repairing the root cause of an incident or problem, or to implement a workaround. This is the measure for Resolved status and SLA measurement. If a workaround is applied a Problem ticket will be raised by Supplier to investigate, replicate, fix, test and ready the fix for deployment into Buyer's UAT environment and support deployment into Production when approved by Buyer.
"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels. Service Credits shall only be applicable three months after the service has exited the Early Life Support (ELS) period.

Early Life Support	a period of two (2) weeks from the Operational Service Commencement Date for each Service.
"Service Credit Cap"	20% of the annual Service Charge
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you don't meet the Service Levels

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(c) results in the corruption or loss of any Government Data; and/or

(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service

Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and

2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

[REDACTED]

Service Level ID	Service Level		Service Level Performance Measure	Service Level Threshold	Maximum Service Credit per Service Level per Service Period
1	Availability of Service	The production platform must be available for a minimum of 99.9% of time for the Core Service Operating Hours (08:00 to 20:00)	Percentage of uptime during Core Service Operating Hours	99.9%	10%
2	P1 incident - Response	Response from the Supplier to the Buyer to a report of a potential P1 incident in <=30 minutes (excluding automated responses).	100% of incidents responded to in <=30 minutes (excluding automated responses) during Primary Operational Support Service Hours	80%	10%
3	P1 incident - Resolution	Resolution of the P1 incident as agreed by the Buyer in <=4 hours during Primary Operational Support Hours	98% Resolved <=4 hours during Primary Operational Support Service Hours	75%	10%
4	P1 incident – Update	Update sent every 30 minutes during Primary Operational Support Service Hours	98% of P1 incidents have updates sent during Primary Operational Support Service Hours mins until resolution	70%	10%

Service Level ID	Service Level		Service Level Performance Measure	Service Level Threshold	Maximum Service Credit per Service Level per Service Period
5	P2 incident - Response	Response from the Supplier to the Buyer to a report of a potential P2 incident in <=60 minutes (excluding automated responses).	100% Responded in <=60 minutes (excluding automated responses) during Primary Operational Support Service Hours	80%	10%
6	P2 incident Resolution	Resolution of the P2 incident as agreed by the Buyer in <=8 hours during Primary Operational Support Service Hours	98% Resolved in <=8 hours during Primary Operational Support Service Hours	75%	10%
7	P2 incident Update	Update sent every 4 hours during Primary Operational Support Service Hours on a P2 incident until Resolution	98% of P2 incidents have updates sent during Primary Operational Support Service Hours every 4 hours until Resolution	70%	10%

Service Level ID	Service Level		Service Level Performance Measure	Service Level Threshold	Maximum Service Credit per Service Level per Service Period
8	P3 incident – Response	Response from the Supplier to the Buyer to a report of a potential P3 incident in <=8 hours (excluding automated responses).	100% Responded to in <=8 hours (excluding automated responses) during Primary Operational Support Service Hours	80%	10%
9	P3 incident – Resolution	Resolution of the P3 incident as agreed by the buyer in <=3 business days during Primary Operational Support Service Hours	98% Resolved in <=3 business days during Primary Operational Support Service Hours	80%	10%
10	P3 Incident Update	Update sent daily during Primary Operational Support Service Hours	98% of P3 incidents have updates sent daily during Primary Operational Support Service Hours until Resolution	70%	10%
11	P4 Service Request- Response	Response from the Supplier to the Buyer to a request for a P4 Service Request in <=2 business days (excluding automated responses).	100% Responded to in <=2 Business Days	80%	10%

Service Level ID	Service Level		Service Level Performance Measure	Service Level Threshold	Maximum Service Credit per Service Level per Service Period
12	P4 Service Request – Resolution	Resolution of the P4 Service Request in <=36 hours during Primary Operational Support Service Hours under change control and agreed deployment into production	90% Resolved in <=36 Service Hours under change control and agreed deployment into production	80%	10%
13	P4 Service Request- Update	Update sent every two (2) Business Days	90% of P4 Service Requests have updates sent every two (2) Working Days until resolution	70%	10%

Calculation of Service Credits

Service Credit per Service Level

The Service Credit for each Service Level shall be calculated for each Service Period using the following formula:

$$SLPM - AP = \%\ deduction$$

Where:

SLPM = Service Level Performance Measure
AP = Actual performance against that Service Level in the Service Period as evidenced by [x]
% deduction = % of the Service Charges to be deducted as a Service Credit subject to the Maximum Service Credit per Service Level per Service Period.

Service Credit per Service Period

The % deduction which forms the Service Credit for each Service Level shall be added together for all the Service Levels to calculate the overall total % deduction as Service Credits for each Service Period and subject to a maximum deduction of the Monthly Service Credit Cap.

Worked example 1:

In this scenario, in the Service Period the Supplier has not met the Service Level Performance Measure for 2 Service Levels (ID2 and ID6) and has met the Service Level Performance Measure for all other Service Levels:

P1 Incidents – Response

Service Level Performance Measure: *100% P1 Incidents Responded to within 15 minutes for the Service as evidenced by the ServiceNow Report*

Actual Performance: *85% P1 Incidents Responded to within 15 minutes for the Service as evidenced by the ServiceNow Report*
% deduction = 15% capped at 10% which forms the Service Credit for this Service Level

P2 Incidents – Resolution

Service Level Performance Measure: *98% Resolved within 8 hours for the Service as evidenced by the ServiceNow Report*

Actual Performance: *96% P2 Incidents Resolved within 8 hours for the Service as evidenced by the ServiceNow Report*
% deduction = 2% which forms the Service Credit for this Service Level
The overall total % deduction applied to the Service Charges for this Service Period is 12%

Worked Example 2:

In this scenario, in the Service Period the Supplier has not met the Service Level Performance Measure for 3 Service Levels (ID2, ID6 and ID7) and has met the Service Level Performance Measure for all other Service Levels:

P1 Incidents – Response (ID2)

Service Level Performance Measure: *100% P1 Incidents Responded to within 15 minutes for the relevant Service Component as evidenced by the ServiceNow Report*

Actual Performance: *83 % P1 Incidents Responded to within 15 minutes for the relevant Service Component as evidenced by the ServiceNow Report*
% deduction = 17% of the Charges related to the affected Service Component, capped at 10%

P2 Incidents – Resolution (ID6)
Service Level Performance Measure: *98% Resolved within 8 hours for the relevant Service Component as evidenced by the ServiceNow Report*

Actual Performance: *90 % P2 Incidents Resolved within 8 hours for the relevant Service Component as evidenced by the ServiceNow Report*

% deduction = 8%

P2 Incidents – Resolution (ID7)
Service Level Performance Measure: *98% updates provided within 60minutes for the relevant Service Component as evidenced by the ServiceNow Report*

Actual Performance: *96 % P2 Incidents updates provided within 60 minutes for the relevant Service Component as evidenced by the ServiceNow Report*
% deduction = 2%

The % deduction applied to the charges for the affected Service Component is 27% but rounded down as per the Monthly Service Credit Cap to 20%.

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

3.2.3 details of any Critical Service Level Failures;

3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

3.2.6 such other details as the Buyer may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

3.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

3.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

4. Satisfaction Surveys

4.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Call-Off Schedule 15 (Call-Off Contract Management)

1. Definitions

1.1 **In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):**

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;
"Service Delivery Manager"	The manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager or Service Delivery Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

[REDACTED]

Call-Off Schedule 16 (Benchmarking)

1. DEFINITIONS

1.1 In this Schedule, the following expressions shall have the following meanings:

"Benchmark Review"	1 a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value;
"Benchmarked Deliverables"	2 any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule;
"Comparable Rates"	3 the Charges for Comparable Deliverables;
"Comparable Deliverables"	4 deliverables that are identical or materially similar to the Benchmarked Deliverables (including in terms of scope, specification, volume and quality of performance) provided that if no identical or materially similar Deliverables exist in the market, the Supplier shall propose an approach for developing a comparable Deliverables benchmark;
"Comparison Group"	5 a sample group of organisations providing Comparable Deliverables which consists of organisations which are either of similar size to the Supplier or which are similarly structured in terms of their business and their service offering so as to be fair comparators with the Supplier or which, are best practice organisations;
"Equivalent Data"	6 data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group;
"Good Value"	7 that the Benchmarked Rates are within the Upper Quartile; and
"Upper Quartile"	8 in respect of Benchmarked Rates, that based on an analysis of Equivalent Data, the Benchmarked Rates, as compared to the range of prices for Comparable

	Deliverables, are within the top 25% in terms of best value for money for the recipients of Comparable Deliverables.

2. When you should use this Schedule

2.1 The Supplier acknowledges that the Buyer wishes to ensure that the Deliverables, represent value for money to the taxpayer throughout the Contract Period.

2.2 This Schedule sets to ensure the Contracts represent value for money throughout and that the Buyer may terminate the Contract by issuing a Termination Notice to the Supplier if the Supplier refuses or fails to comply with its obligations as set out in Paragraphs 3 of this Schedule.

2.3 Amounts payable under this Schedule shall not fall with the definition of a Cost.

3. Benchmarking

3.1 How benchmarking works

3.1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

3.1.2 The Buyer may, by written notice to the Supplier, require a Benchmark Review of any or all of the Deliverables.

3.1.3 The Buyer shall not be entitled to request a Benchmark Review during the first six (6) Month period from the Contract Commencement Date or at intervals of less than twelve (12) Months after any previous Benchmark Review.

3.1.4 The purpose of a Benchmark Review will be to establish whether the Benchmarked Deliverables are, individually and/or as a whole, Good Value.

3.1.5 The Deliverables that are to be the Benchmarked Deliverables will be identified by the Buyer in writing.

3.1.6 Upon its request for a Benchmark Review the Buyer shall nominate a benchmarker. The Supplier must approve the nomination within ten (10) Working Days unless the Supplier provides a reasonable explanation for rejecting the appointment. If the appointment is rejected then the Buyer may propose an alternative benchmarker. If the Parties cannot agree the appointment within twenty (20) days of the initial request for Benchmark review then a benchmarker shall be selected by the Chartered Institute of Financial Accountants.

3.1.7 The cost of a benchmarker shall be borne by the Buyer (provided that each Party shall bear its own internal costs of the Benchmark Review) except where the Benchmark Review

demonstrates that the Benchmarked Service and/or the Benchmarked Deliverables are not Good Value, in which case the Parties shall share the cost of the benchmarker in such proportions as the Parties agree (acting reasonably). Invoices by the benchmarker shall be raised against the Supplier and the relevant portion shall be reimbursed by the Buyer.

3.2 **Benchmarking Process**

3.2.1 The benchmarker shall produce and send to the Buyer, for Approval, a draft plan for the Benchmark Review which must include:

(a) a proposed cost and timetable for the Benchmark Review;

(b) a description of the benchmarking methodology to be used which must demonstrate that the methodology to be used is capable of fulfilling the benchmarking purpose; and

(c) a description of how the benchmarker will scope and identify the Comparison Group.

3.2.2 The benchmarker, acting reasonably, shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking.

3.2.3 The Buyer must give notice in writing to the Supplier within ten (10) Working Days after receiving the draft plan, advising the benchmarker and the Supplier whether it Approves the draft plan, or, if it does not approve the draft plan, suggesting amendments to that plan (which must be reasonable). If amendments are suggested then the benchmarker must produce an amended draft plan and this Paragraph 3.2.3 shall apply to any amended draft plan.

3.2.4 Once both Parties have approved the draft plan then they will notify the benchmarker. No Party may unreasonably withhold or delay its Approval of the draft plan.

3.2.5 Once it has received the Approval of the draft plan, the benchmarker shall:

(a) finalise the Comparison Group and collect data relating to Comparable Rates. The selection of the Comparable Rates (both in terms of number and identity) shall be a matter for the Supplier's professional judgment using:

(i) market intelligence;

(ii) the benchmarker’s own data and experience;

(iii) relevant published information; and

(iv) pursuant to Paragraph 3.2.6 below, information from other suppliers or purchasers on Comparable Rates;

(b) by applying the adjustment factors listed in Paragraph 3.2.7 and from an analysis of the Comparable Rates, derive the Equivalent Data;

(c) using the Equivalent Data, calculate the Upper Quartile;

(d) determine whether or not each Benchmarked Rate is, and/or the Benchmarked Rates as a whole are, Good Value.

3.2.6 The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the benchmarker in order to undertake the benchmarking. The Supplier agrees to use its reasonable endeavours to obtain information from other suppliers or purchasers on Comparable Rates.

3.2.7 In carrying out the benchmarking analysis the benchmarker may have regard to the following matters when performing a comparative assessment of the Benchmarked Rates and the Comparable Rates in order to derive Equivalent Data:

(a) the contractual terms and business environment under which the Comparable Rates are being provided (including the scale and geographical spread of the customers);

(b) exchange rates;

(c) any other factors reasonably identified by the Supplier, which, if not taken into consideration, could unfairly cause the Supplier's pricing to appear non-competitive.

3.3 **Benchmarking Report**

3.3.1 For the purposes of this Schedule **"Benchmarking Report"** shall mean the report produced by the benchmarker following the Benchmark Review and as further described in this Schedule;

3.3.2 The benchmarker shall prepare a Benchmarking Report and deliver it to the Buyer, at the time specified in the plan Approved pursuant to Paragraph 3.2.3, setting out its findings. Those findings shall be required to:

(a) include a finding as to whether or not a Benchmarked Service and/or whether the Benchmarked Deliverables as a whole are, Good Value;

(b) if any of the Benchmarked Deliverables are, individually or as a whole, not Good Value, specify the changes that would be required to make that Benchmarked Service or the Benchmarked Deliverables as a whole Good Value; and

(c) include sufficient detail and transparency so that the Party requesting the Benchmarking can interpret and understand how the Supplier has calculated whether or not the Benchmarked Deliverables are, individually or as a whole, Good Value.

3.3.3 The Parties agree that any changes required to this Contract identified in the Benchmarking Report shall be implemented at the direction of the Buyer in accordance with Clause 24 (Changing the contract).

Call-Off Schedule 18 (Background Checks)

1. When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on Contract.

2. Definitions

"Relevant Conviction" means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

3.1.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

3.1.2 Notwithstanding Paragraph 2.1.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

(a) carry out a check with the records held by the Department for Education (DfE);

(b) conduct thorough questioning regarding any Relevant Convictions; and

(c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1 – Relevant Convictions

N/A

Call-Off Schedule 20 (Call-Off Specification)

[REDACTED]

	Abbreviation	Full Name
1	**ALB**	Arm's Length Body
2	**API**	Application Programming Interface
3	**APVU**	Assisted Prison Visiting Unit
4	**ATS**	Applicant Tracking System
5	**BOM**	Bill of Materials
6	**BPS**	Business Process Outsourcing
7	**BSV**	Balancing Segment Value
8	**CAFCASS**	The Children and Family Court Advisory and Support Service
9	**CCRC**	Criminal Cases Review Commission
10	**CDDO**	Central Digital and Data Office
11	**CIA**	Change Impact Assessment
12	**CICA**	Criminal Injuries Compensation Authority
13	**CMA**	Case Management Application
14	**CMS**	Case Management System
15	**CoA**	Chart of Accounts
16	**COTS**	Commercial Off The Shelf
17	**CRM**	Customer Relationship Management
18	**CTS**	Courts and Tribunals Service (shorthand for HMCTS)
19	**DIS**	Data Integration Service
20	**DRM**	Data Relationship Manager
21	**E2E**	End to End
22	**eLinks**	API platform used to make JOH data from Judicial HR available for ingesting by third
23	**ePM**	Electronic Performance Management
24	**ERP**	Enterprise Resource Planning
25	**FOI**	Freedom of Information
26	**FSG**	Financial Statement Generator
27	**GDPR**	General Data Protection Regulation
28	**GDS**	Government Digital Service
29	**GPC**	Government Procurement Card
30	**GSR**	Generic Service Request
31	**HCM**	Human Capital Management
32	**HMCTS**	His Majesty's Courts and Tribunals Service
33	**HMPPS**	His Majesty's Prison and Probation Service
34	**HMT**	His Majesty's Treasury
35	**HR**	Human Resources
36	**HRP**	Human Resources Payroll

37	**HTTPS**	Hypertext Transfer Protocol Secure
38	**ICGC**	Investment and Commercial Governance Committee
39	**IMA**	Independent Monitoring Authority
40	**IMB**	Independent Monitoring Boards
41	**ITHC**	IT Health Check
42	**ITSM**	IT Service Management
43	**ITT**	Invitation to Tender
44	**JAC**	Judicial Appointments Commission
45	**JCA**	Judicial Conduct Authority
46	**JCL**	Joiners, Changers, Leavers
47	**JCL**	Judicial College Learning
48	**JFEPS**	Justice Fees and Expenses Payment System
49	**JO HR**	Judicial Office Human Resources
50	**JO**	Judicial Office
51	**JOH**	Judicial Office Holder
52	**JPET**	Judicial Pay & Expenses Team
53	**JPP**	Judicial Payroll Project
54	**JPS**	Judicial Pension Scheme
55	**Judicial HR**	HR system used by Judicial Office to manage JOH personal and appointment data
56	**LAA**	Legal Aid Agency
57	**Liberata**	The outsourced provider for the Judicial Payroll
58	**LSB**	Legal Service Board
59	**MDM**	Master Data Management
60	**MI**	Management Information
61	**MoJ**	Ministry of Justice
62	**MRD**	Master and Reference Data
63	**MSP**	Managed Service Provider
64	**NDA**	Non-Disclosure Agreement
65	**NDPB**	Non-Departmental Public Body
66	**NFR**	Non-Functional Requirement
67	**NIO**	Northern Ireland Office
68	**NLM**	Non Legal Member
69	**NMS**	National Offender Management Service
70	**OBC**	Outline Business Case
71	**OCI**	Oracle Cloud Infrastructure
72	**OPG**	Office of the Public Guardian
73	**OSCAR**	The Online System for Central Accounting and Reporting
74	**PB**	Parole Board
75	**PMO**	Project Management Office
76	**POAP**	Proof of Attendance Protocol
77	**RAID**	Risks, Actions, Issues and Decisions
78	**RCJ**	Royal College of Justice
79	**Regional Offices**	Any local court/tribunal administrative function that provides data for payroll

80	**REST**	Representational State Transfer
81	**ROC**	Remuneration of Costs
82	**SaaS**	Software as a Service
83	**SDAT**	Service Design and Transition
84	**SEND**	Special Educational Needs and Disability
85	**SFTP**	Secure File Transfer Protocol
86	**SOAP**	Simple Object Access Protocol
87	**SOP**	Software on Premise
88	**SoW**	Statement of Work
89	**SRO**	Senior Responsible Officer
90	**SSCL**	Shared Services Connected Limited
91	**SSCS**	Social Security and Child Support
92	**SSO**	Single Sign-On
93	**TAB**	Technical Architecture Board
94	**TAC**	Trust Accounts
95	**TDA**	Technical Design Authority
96	**TGL**	Technical Guidance Library
97	**TOM**	Target Operating Model
98	**UAT**	User Acceptance Testing
99	**WCAG**	Web Content Accessibility Guidelines
100	**WLS**	Wales Office (abbreviation often used in SOP)
101	**YJB**	Youth Justice Board

1. SCOPE OF REQUIREMENT

1.1. Business Outcomes

1.1.1. HMCTS Digital and Technology Services (DTS) are looking for a supplier to deliver a single software solution to replace the current JFEPS.

1.1.2. Due to the issues the lack configurability has caused with the functionality of JFEPS, HMCTS are looking for a single software solution which will allow for basic reconfigurability by HMCTS staff as detailed in the Functional Requirements document.

1.2. The main Business Outcomes are as follows:

1.2.1. Provide self-service functionality for Judicial Office Holders to manage their own fee and expense claims.

1.2.2. Streamline existing business-required capabilities by introducing seamless integration and automation wherever possible.

1.2.3. Automate administrative processes as much as possible, including managing bulk imports and user accounts.

1.2.4. Ingest source data using the current JFEPS processes and interfaces.

1.2.5. Support the transition away from existing manual JFEPS processes to automated processes by introducing API capability.

1.2.6. Provide the capability for System Administrators to manage business rules, including automated expense claim validation and fee calculations.

1.2.7. Output files to Liberata and SSCL using the current JFEPS formats.

1.2.8. Provide capability for System Administrators to define new file formats for output to third party suppliers as required.

1.2.9. Migration of current data to the new JFEPS system

4.3 The following points provide additional context to the current processes and systems behind the required business outcomes:

4.3.1 Most Expense claims and some Fee claims are raised via an end-user self-service portal and are verified against corroborating data received in Excel/CSV format from across the different Tribunals/Jurisdictions.

4.3.2 Most Fee claims are manually imported in bulk using output files from other HMCTS systems that record Judicial Office Holder sittings in the various Tribunals. Some Fee claims that are processed in bulk, including those for Courts, currently bypass the current system and are manually compiled in Excel.

4.3.3 Claims are also subject to validation against the MoJ Fees and Expenses policies.

4.3.4 Some of these policies are automated within the current core system, or within a component of the current system which is a secondary product with additional functionality.

4.3.5 Many validation processes are performed manually, comparing data in the current system with data shown on other screens or spreadsheets.

4.3.6 The current system comprises two main products which are partially integrated; however, because data has to maintained in both products, there are occasional mismatches. These have to be identified via a mismatch process using a third product.

4.3.7 The combination of products, limited integration, separation of data and functionalities, and the significant manual effort involved has resulted in a system which cannot achieve the required level of operational accuracy to meet operational timelines.

1.3. Out of Scope

1.3.1. The decommissioning of the existing JFEPS system will not be within the scope of the new contract. This will be the responsibility of the incumbent and HMCTS to manage and undertake.

2. THE REQUIREMENT

2.1. The HMCTS Judicial Fees and Expenses System requirements are as follows:

2.1.1. The embedded files contain details of the following sets of requirements:

2.1.1.1. Compliance Must Haves JFEPS Functional Requirements (detail in Annex B HMCTS Requirements)

[REDACTED]

2.2. Compliance Must Haves JFEPS NFR's (detail in Annex B HMCTS Requirements)

[REDACTED]

2.3. JFEPS Functional Requirements (detail in Annex B HMCTS Requirements)

[REDACTED]

2.4. JFEPS Non-Functional Requirements (detail in Annex B HMCTS Requirements)

[REDACTED]

2.5. Volumetric specification (Transaction Time Analysis and Data Migration Outline) (detail in Annex B HMCTS Requirements)

[REDACTED]

2.6. HMCTS Security Non-Functional Requirements (detail in Annex B HMCTS Requirements)

[REDACTED]

5.2 SERVICE DELIVERY REQUIREMENTS

2.7. 5.2.1 Staff and Buyer Service

2.8. 5.2.1.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract to consistently deliver a quality service.

2.9. 5.2.1.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

2.10. 5.2.1.3 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent service to the Buyer throughout the duration of the Contract.

2.11. 5.2.2 Data Handling and Validation

2.12. 5.2.2.1 The Supplier must ensure all referential data integrity and data relationships are preserved during the extract, transform and load (ETL) process.

2.13. 5.2.2.2 Appropriate measures will be put in place by the supplier to ensure the confidentiality and integrity of sensitive data during the migration process.

2.14. 5.2.2.3 Development of the specification of data extracts to be carried out by the supplier.

2.15. 5.2.2.4 Physical, secure transfer of extract data from source systems in multiple organisations to the location where the validation and loading process is to be undertaken by the Supplier.

2.16. 5.2.2.5 Regular refreshing of extract data will be completed by the Supplier, to support a refresh schedule throughout the lifetime of the Framework Contract and any Call-Off Contracts.

2.17. 5.2.2.6 The Supplier will manage the continuous improvement of data quality, through an iterative cleansing and the mapping process.

2.18. 5.2.2.7 The Supplier will build, operate, host and maintain an analysis database ensuring that it is appropriately structured and optimised and has sufficient hardware resources to operate efficiently and effectively and loading all extract data into this analysis database.

2.19. 5.2.3 Disaster Recovery and Backup Services

2.20. 5.2.3.1 The Supplier must provide services including Backup as a Service and Disaster Recovery as a Service

2.21. 5.2.3.2 The Supplier will conduct monitoring, reporting and analytics.

2.22. 5.2.3.3 The Supplier will be expected to align to ITIL Event management standards.

2.23. 5.2.3.4 The Supplier must commit to providing a Recovery Point Objective (RPO) of no more than 4 hours and a Recovery Time Objective (RTO) of no more than 4 hours.

2.24. 5.2.4 Standards and Accreditations

2.25. 5.2.4.1 The Supplier shall at all times comply with relevant Standards for Service Management including ISO/IEC 20000-1 2018 “ITSM Specification for Service Management” or equivalent.

2.26. 5.2.4.2 The Supplier shall at all times comply with relevant Standards for Service Management including ISO ISO27031 “Security techniques — Guidelines for information and communication technology readiness for business continuity, ensuring they develop, maintain and provide an up to date ITSCM Plan.

2.27. 5.2.4.3 The Supplier shall at all times comply with relevant Standards for Service Management including ISO 10007:2017 “Quality management systems – Guidelines for configuration management”.

2.28. 5.2.4.4 The Supplier shall at all times comply with the HMCTS’s open standard principles as detailed in: https://www.gov.uk/government/publications/open-standards-principles.

2.29. 5.2.4.5 The Supplier shall at all times comply with Government open data standards as detailed in: https://www.gov.uk/government/publications/open-standards-for-government.

2.30. 5.2.4.6 The Supplier shall at all times comply with the HMCTS's Technology code of practice detailed in: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

2.31. 5.2.5 Hosting Services

2.32. 5.2.5.1 The Supplier will provide development, test, and live (production) environments.

2.33. 5.2.5.2 The Supplier shall manage the system infrastructure, including performance and management of the central server configuration, encryption management, firewall management, data filter management and WAN management.

2.34. 5.2.5.3 The Supplier shall proactively monitor the system servers and related network for traffic and capacity, and reporting on traffic volumes, disk utilisation and percentage capacity free on disk, performance data, workload analysis, peaks and failures for each reporting period.

2.35. 5.2.6 Software and Support and Maintenance

2.36. 5.2.6.1 The Supplier will develop, test and implement all necessary updates to ensure that the software undertakes all processing to include changes to the taxation regime applied by HMRC, changes to law by legislators and changes in regulation by regulatory bodies (or such bug fixes where available from the relevant software owner advisory services in the implementation thereof)

2.37. 5.2.6.2 The Supplier shall monitor the operation of the software in order to assure application and information availability and integrity.

2.38. 5.2.6.3 The Supplier will provide a knowledge-base of known issues and solutions in respect of the software.

2.39. 5.2.6.4 The Supplier will provide release notes to customers.

2.40. 5.2.6.5 The Supplier will provide operational support as part of their application management service;

2.41. 5.2.6.6 The Supplier may provide management of updates and patches related to software purchased via this Framework Contract.

2.42. 5.2.7 Implementation

2.43. In addition to the obligations set out in Call-Off Schedule 13 (Implementation Plan and Testing) the following requirements apply:

2.44. 5.2.7.1 The Implementation Plan must include a detailed RACI (Responsible, Accountable, Consulted, Informed) matrix based in part on Buyer input.

2.45. 5.2.7.2 The Implementation Plan must include key Milestone dates laid out by the Buyer in Annex 1 of the Call-Off Schedule 13 (Implementation Plan and Testing), and should incorporate activities, Deliverables and Milestones associated with aspects including technical, service, commercial, finance, people and testing.

2.46. 5.2.7.3 The Supplier shall build and configure the solution in line with the specified requirements and approved designs including the technical and service designs.

2.47. 5.2.7.4 In accordance with the Call-Off Schedule 13 (Implementation Plan and Testing), the Supplier shall undertake appropriate Service Management, user acceptance and end to end (unstructured) Testing of Services with the Buyer's delivery team and Services to ensure that their solution and operation of the scope of Services is ready for all required Operational Service Commencement Dates and supporting rectification of Test Issues before the relevant Operational Service Commencement Date of each Service. The Supplier shall be responsible for supporting the Buyer in the planning, design, implementation, execution and reporting of the Service Management, user acceptance and end to end Testing.

2.48. 5.2.7.5 Deployment Plan

2.49. 5.2.7.5.1 The Supplier to produce a Deployment Plan to ensure that the system is ready for distribution, focusing on a smooth transition and minimal disruption during implementation. The Plan will include the methods and procedures to be used for deployment.

2.50. 5.2.7.6 Training Plan

2.51. 5.2.7.6.1 The Supplier shall provide the Buyer with a training approach and plan which shall include:

2.52. 5.2.7.6.2 analysis of training needs and subsequent identification of appropriate training; and

2.53. 5.2.7.6.3 the Supplier approach to meeting the training needs including:

2.54. 5.2.7.6.4 how training materials will be developed; and

2.55. 5.2.7.6.5 The Supplier shall produce and agree with the Buyer suitable training material and knowledge articles for, and undertake training with, the relevant team leader, agents and administrators.

2.56. 5.2.7.7 Cutover Plan

2.57. 5.2.7.7.1 The Supplier shall provide to and seek approval from the Buyer for a Cutover Plan(s) that covers the pre- and post- period of Operational Service Commencement Date for each of the Services and includes:

2.58. 5.2.7.7.2 the activities required to transition each Service;

2.59. 5.2.7.7.3 the timings and resources required to cutover from the Preceding Services to the Services; and

2.60. 5.2.7.7.4 a level of detail which provides the Buyer with assurance on the Supplier ability to meet Operational Service Commencement Dates.

2.61. 5.2.7.8 Service Transition and Early Life Support

2.62. 5.2.7.8.1 The Supplier shall engage and comply with a joint Transition governance forum including:

2.63. 5.2.7.8.2 jointly undertake the governance of the Transition;

2.64. 5.2.7.8.3 confirm the Transition Milestone completion and to act as an escalation point;

2.65. 5.2.7.8.4 select an escalation group in case the joint Transition governance cannot resolve all issues;

2.66. 5.2.7.8.5 deal with all aspects of Preceding Services, Other Suppliers, site-cooperation, information exchanges;

2.67. 5.2.7.8.6 deal with technical and business change required;

2.68. 5.2.7.8.7 discuss changes requested by the Supplier or the Buyer;

2.69. 5.2.7.8.8 meeting regularly at a specified cadence; and

2.70. 5.2.7.8.9 issue meeting minutes.

2.71. 5.2.7.9 The Supplier to assign a transition lead, who will:

2.72. 5.2.7.9.1 Manage the Supplier responsibilities within the Transition;

2.73. 5.2.7.9.2 Supervise the conduct of the Transition on behalf of the Supplier;

2.74. 5.2.7.9.3 Take full accountability for the Transition delivery on behalf of the Supplier;

2.75. 5.2.7.9.4 Liaise with the Buyer on behalf of the Supplier;

2.76. 5.2.7.9.5 Provide assistance to the Buyer's Transition manager in the communication with and coordination of the Buyer's resources required to achieve the Transition;

2.77. 5.2.7.9.6 Ensure a communication plan and assist the Buyer's Transition manager in communicating with both end users and the Buyer's stakeholders;

2.78. 5.2.7.9.7 Maintain all Transition project records including logs for Transition incidents, risks and issues.

2.79. 5.2.8 For a period of two (2) weeks from the Operational Service Commencement Date for each Service, the Supplier will provide Early Life Support, to resolve operational and support issues quickly and reduce the amount of unavailability.

2.80. 5.2.9 To exit Early Life Support, the acceptance process will be complete, executing service transfer plans and service readiness confirmed by the buyer.

2.81. 5.2.10 Service Desk

2.82. In addition to the Service Levels and Performance identified in Call Off Schedule 14 Service Levels:

2.83. 5.2.10.1 The Supplier will provide a Service Desk to act as a single point of contact for the Customer or its nominated representatives, ensuring that issues are effectively progressed and resolved, and provide information on the impact of planned changes and unplanned events.

2.84. 5.2.10.2 The Supplier will provide 3rd line support for resolution of Service incidents and problems that meets the requirements of the specified Service Level Targets.

2.85. 5.2.10.3 Primary operational support service hours are defined as 08:00 to 18:00 (GMT/BST). Secondary service hours are defined as 18:00 to 08:00 (GMT/BST). Service must be supported during the Core Service Operating Hours 08:00 to 20:00 (GMT/BST). Services must be available to end users during secondary service hours but will be limited.

2.86. 5.2.10.4 The Supplier must define, document and agree with the Authority the roles and responsibilities of their staff and Subcontractors who are responsible for delivering, administering and operating the Solution.

2.87. 5.2.10.5 The Supplier must co-operate with any other service provider notified to them by the buyer from time to time by providing: (i) reasonable information (including any Documentation); (ii) advice; and (iii) reasonable assistance (in connection with the services procured) to any such other service provider to enable them to create and maintain technical or organisational interfaces.

2.88. 5.2.11 Service Management

2.89. 5.2.11.1 The Supplier to provide support, as defined and agreed between both parties, in order to maintain their Service Management Policies, Processes and Procedures. Where possible, the Supplier will adapt to any changes made to HMCTS Service Management Policies, Processes and Procedures throughout the Call-Off Contract Period that are relevant to the service and are agreed through the Governance Framework.

2.90. 5.2.11.2 The Supplier to measure suitable incident, problem and change process performance KPIs for the agreed reporting period and in line with service levels within Call-Off Schedule 14 (Service Levels).

2.91. 5.2.11.3 The Supplier will facilitate a recurring quarterly Service review meetings during normal operation and will present the Service performance report. The service report should be ready and sent for review 5 working days before the quarterly service review meeting.

2.92. 5.2.11.4 The Supplier will facilitate a recurring monthly Service review meetings during Continuous Service Improvement (CSI) projects and will present the Service performance report. The service report should be ready and sent for review 5 working days before the monthly quarterly service review meeting.

2.93. 5.2.12 Incident Management

2.94. 5.2.12.1 The Supplier shall undertake tests to identify the nature of the reported Incident and the results will be passed to HMCTS as appropriate. If such results indicate a potential Incident within any element of the

Service, Supplier will initiate appropriate further diagnostic and/or Incident repair activity.

2.95. 5.2.12.2 The Supplier to provide an incident response plan(s) for any host-related incidents to minimize downtime.

2.96. 5.2.12.3 The Supplier should provide incident root cause analysis information within 10 working days.

2.97. 5.2.12.4 The Supplier's major incident management to align with the ITIL V4 and update communications according to service level agreement.

2.98. 5.2.13 Change Management

2.99. 5.2.13.1 The Supplier's handling and implementation of Change Requests must be subject to a management process that provides the Customer with appropriate control of expenditure, risk, implementation of policies and strategy (Change Management) using a process which is in with ITIL V4 Service Management best practice.

2.100. 5.2.13.2 The Supplier shall ensure that all Requests for Change they submit contain information including but not limited to: (i) Verified Implementation Plans; (ii) Post Implementation Review; (iii) Acceptance Criteria; (iv) Back Out Plans or Remediation Plans; (v) Plans for handover to support; and (vi) Evidence of successful test activity.

2.101. 5.2.13.3 Changes to the Platform and Applications (other than those which are straightforward or routine and bear little risk) must be managed by the Supplier under a process that is designed to minimise risk and the impact on normal service (Release Management) and which is in line with ITIL V4 Service Management best practice.

2.102. 5.2.13.4 The Supplier shall receive Change Requests from the Customer or its nominated representative and will provide an Impact Analysis on such requests back to the Customer or it's nominated representative within a maximum of 5 days.

2.103. 5.2.13.5 Where there are any changes to software, the Supplier is to inform the buyer within a reasonable notice period in order to impact assess and mitigate any risks.

2.104. 5.2.13.6 The Supplier is required to perform maintenance and upgrades outside core operating hours, ensuring service and data integrity through resilient deployment methods. Rigorous pre-deployment testing is mandatory, and any unplanned critical patches must be applied within specific timeframes to maintain service continuity.

2.105. 5.2.13.7 Where unplanned maintenance and patches are required for any platform component, the patch will be applied within

2.106. 5.2.13.7.1 Four (4) hours, where it fixes a critical security flaw

2.107. 5.2.13.7.2 Seven (7) days, where it provides stability improvements

2.108. 5.2.13.7.3 Six (6) weeks, where it provides new functionality.

2.109. 5.2.14 Problem

2.110. 5.2.14.1 The Supplier to align to ITIL problem management process, including the provision of problem identification details, root cause analysis information, and resolution plan.

2.111. 5.2.14.2 The Supplier to present new and existing Problem tickets raised, current status and resolution times.

2.112. 5.2.14.3 Services should capture variance in performance between releases and have a plan in place to address and performance degradation.

2.113. 5.2.14.4 The Supplier shall, for the duration of the service and agreed period thereafter, provide historical access to Performance Monitoring Reports as required by HMCTS.

2.114. 5.2.15 Continuous Service Improvement

2.115. 5.2.15.1 The Supplier and HMCTS will bring to the table Service improvement initiatives which will be tracked by the Supplier until implemented. The Supplier will maintain Continuous Service Improvement CSI register and Risk Management risk register. The Supplier will also respond to the HMCTS's requests for enhancements in line with the service level agreement.

2.116.

2.117. 5.3 Dependencies and Assumptions

Table 3

DEPENDENCY	**ASSUMPTION**
Supplier will have a dependency on the incumbent JFEPS provider, and other	Supplier will be required to work cooperatively and in partnership with the incumbent supplier, and other Supplier(s)

DEPENDENCY	ASSUMPTION
internal data teams, to successfully deliver data migration.	where applicable. Ways of working will be supported by HMCTS project and product teams.
Ability to align to intended implementation schedule as multiple parties will need to be involved in agreement and coordination of testing, data migration and implementation approach. HMCTS Finance team have to manage BAU activity in tandem with the development of the new service.	Clear plans to be agreed, close partnership across all internal HMCTS teams and suppliers. Robust project management with tracking of risks and issues and mitigation as these arise. HMCTS resource availability to be prioritised.

5.5 Buyer Responsibilities

[REDACTED]

Table 4

3. KEY MILESTONES AND DELIVERABLES

3.1. In line with the milestones set out on Call-Off Schedule 13 (Implementation Plan and Testing) the following Contract deliverables shall apply:

Table 51

Deliverable ID	Deliverable	Description	Timeframe or Delivery Date
1	Contract	New Contract approved and signed.	

Deliverable ID	Deliverable	Description	Timeframe or Delivery Date
2	Initiation Document	To include: • a section detailing transition objectives and outcomes; • a section detailing the scope; • a section detailing the approach; • a section detailing key activities; • a section detailing key assumptions; • a section detailing the team organisational structure; • a section outlining the key stakeholders and communication strategy approach; • a section outlining the change management approach; • a section detailing the transition project controls.	

Deliverable ID	Deliverable	Description	Timeframe or Delivery Date
3	Implementation Plan	To include: • detail of all key implementation activities; • draft technical, service and operational process flows as required; • critical path including the Transition Milestones as detailed in Call-Off Schedule 13, Annex 1; • detail of the required personnel resources per section; • detail of the impact on the service continuity of Services; • detail of the impact on the general operation of the Services business; • detail of the impact on any connected In-flight projects; • RACI (Responsible, Accountable, Consulted, Informed) matrix; • Identification and agreement of any dependencies on the Buyer and/or the Buyer's stakeholders and/or Other Suppliers including providers of Preceding Services; • Data Migration Plan. To be Built in a way that progress against each task can be reported to the Buyer and reported as necessary.	

Deliverable ID	Deliverable	Description	Timeframe or Delivery Date
4	Test Strategy	As detailed in part B, section 3, of Call-Off Schedule 13 (Implementation Plan and Testing).	
5	Test Plan	As detailed in part B, section 4, of Call-Off Schedule 13 (Implementation Plan and Testing).	
6	Test Reports	As detailed in part B, section 7, of Call-Off Schedule 13 (Implementation Plan and Testing).	
7	Training Plan	To include: • analysis of training needs; • identification of appropriate training; • production of training materials and knowledge articles as required.	
8	Deployment Plan	To include: • the plan for minimising disruption during deployment; • the methods and procedures to be used for deployment.	
9	Cutover Plan	To include: • the activities required to transition each Service; • the timings and resources required to cutover from the Preceding Services to the Services; • a level of detail which provides the Buyer with assurance on the Supplier ability to meet Operational Service Commencement Dates.	

Deliverable ID	Deliverable	Description	Timeframe or Delivery Date
10	Early Life Support Plan	To include: • activities, resources, communications and escalation paths that will occur post Operational Service Commencement Date prior to exit of Early Life Support; • criteria for stabilisation of the Service.	
11	Post Go-Live Review / Lessons Learned	Supplier to participate in and contribute to post Operational Service Commencement Date reviews and lessons learned review for each Service.	

4. SECURITY REQUIREMENTS

4.1. Security Management Plan

4.2. The Supplier is required to provide a Security Management Plan within 20 working days of the contract being signed. The Supplier shall obtain the Customer's approval of, maintain and observe a Security Management Plan and an Information Security Management System (ISMS) which, after the Customers approval, will apply during the term of this Call Off Contract. Both the ISMS and Security Management Plan will comply with the MoJ ICT Security Guide and protect all aspects of the Services and all processes associated with the delivery of the Services.

4.3. Upon the signing of the contract, the Supplier will also be required to complete and provide a signed copy of a Security Aspects Letter (SAL) to the Customer.

4.4. Customers ICT and Security Policy

4.5. The Supplier warrants and undertakes to the Customer that the Supplier and Supplier staff have read and understood the above referenced documents and are able to deliver the Services in accordance with the instructions, practices and standards detailed in the above referenced documents.

4.6. Please refer to https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance for the Security Policy.

5. CONTRACT MANAGEMENT

5.1. Monthly Service reviews to take place between Customer and Supplier Meetings to be arranged by the Supplier Delivery Manager.

5.2. Weekly/fortnightly review meeting to take place between HMCTS Product Manager and Supplier Delivery Manager. Meetings to be arranged by the Supplier Delivery Manager.

5.3. Attendance at Contract Review meetings held at the Customer's permanent office shall be at the Supplier's own expense.

6. LOCATION

6.1. Primary contract locations are:

6.2. **[REDACTED]**

6.3. **[REDACTED]**

6.4. **[REDACTED]**

6.5. It could be necessary for Supplier to travel to additional locations in agreement with the Authority.

SUPPLIER'S TENDER RESPONSE

Question 4.1:

Please describe how the solution would meet the requirements to validate that fee and expense claims meet policy requirements.

[REDACTED]

Question 4.2:

Please explain how the solution would fulfil the complex requirements around differing fee rates for Medical Members based on their "ticket" level and the number of sittings they have undertaken since 6 April.

[REDACTED]

Question 4.3:

Please describe how the solution would fulfil requirements around London Weighting adjustments to payment rates.

[REDACTED]

Question 4.4:

Please explain how the solution would fulfil the requirement for Fee Rates to be bulk updated retrospectively following an annual increase.

[REDACTED]

Question 4.5:

Please describe how the solution would support the requirement to manage recovery of overpayments.

[REDACTED]

Question 4.6:

[REDACTED]

Question 4.7:

Please describe how the solution will meet the reporting requirements.

[REDACTED]

Question 4.8:

Please describe how the solution will support the requirements around holding 'person' and 'appointment' data and its various associated attributes.

[REDACTED]

Question 4.9:

Please describe how the solution will meet the requirements around self-service claims and approvals, and associated supporting functionality.

[REDACTED]

Question 4.10:

Please describe how the solution will meet the requirements around administration and configurability.

[REDACTED]

Question 4.11:

Please provide a draft implementation plan for successfully configuring, testing and transitioning the solution in accordance with the Buyer's requirements.

[REDACTED]

Question 4.12:

Please describe the service management provision that you will deliver in association with the system.

Please outline the approach to service management, performance management, and associated reviews and reporting.

[REDACTED]

Question 4.13: **Fighting Climate Change**

[REDACTED]

Call-Off Schedule 23 (Supplier-Furnished Terms)

[REDACTED]

Annex 1

Not applicable

Annex 2

Not applicable

Annex 3

See: Annex A – SalesForce Main Service Agreement

Annex 4

Not applicable

CCS Core Terms (Version 3.0.10)

[REDACTED]

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any

allegation of slavery or human trafficking offenses anywhere around the world.

3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.

3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;

3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;

4.1.3 All workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

5.1.3 ensure that use of overtime used responsibly, taking into account:

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

1.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

1.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

1.3.1 this is allowed by national law;

1.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

appropriate safeguards are taken to protect the workers' health and safety; and

1.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

1.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

2. Sustainability

2.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

Call-Off Schedule 4 (Call Off Tender) NOT USED

Annex A – SalesForce Main Service Agreement

MAIN SERVICES AGREEMENT

THIS MAIN SERVICES AGREEMENT GOVERNS CUSTOMER'S ACQUISITION AND USE OF SFDC SERVICES. CAPITALIZED TERMS HAVE THE DEFINITIONS SET FORTH HEREIN.

IF CUSTOMER REGISTERS FOR A FREE TRIAL OF SFDC SERVICES OR FOR FREE SERVICES, THE APPLICABLE PROVISIONS OF THIS AGREEMENT WILL ALSO GOVERN THAT FREE TRIAL OR THOSE FREE SERVICES.

BY ACCEPTING THIS AGREEMENT, BY (1) CLICKING A BOX INDICATING ACCEPTANCE, (2) EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, OR (3) USING FREE SERVICES, CUSTOMER AGREES TO THE TERMS OF THIS AGREEMENT. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, SUCH INDIVIDUAL REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERM "CUSTOMER" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT DOES NOT HAVE SUCH AUTHORITY, OR DOES NOT AGREE WITH THESE TERMS AND CONDITIONS, SUCH INDIVIDUAL MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SERVICES.

The Services may not be accessed for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes.

SFDC's direct competitors are prohibited from accessing the Services, except with SFDC's prior written consent.

This Agreement was last updated on October 16, 2023. It is effective between Customer and SFDC as of the date of Customer's accepting this Agreement (the "Effective Date").

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Agreement**" means this Main Services Agreement.

"**Beta Services**" means SFDC services or functionality that may be made available to Customer to try at its option at no additional charge which is clearly designated as beta, pilot, limited release, developer preview, non-production, evaluation, or by a similar description.

"**Content**" means information obtained by SFDC from publicly available sources or its third-party content providers and made available to Customer through the Services, Beta Services or pursuant to an Order Form, as more fully described in the Documentation.

"**Customer**" means in the case of an individual accepting this Agreement on his or her own behalf, such individual, or in the case of an individual accepting this Agreement on behalf of a company or other legal entity, the company or other legal entity for which such individual is accepting this Agreement, and Affiliates of that company or entity (for so long as they remain Affiliates) which have entered into Order Forms.

"**Customer Data**" means electronic data and information submitted by or for Customer to the Services, excluding Content and Non-SFDC Applications.

"**Documentation**" means the applicable Service's Trust and Compliance documentation at https://www.salesforce.com/company/legal/trust-and-compliance-documentation/ and its usage guides and policies, as updated from time to time, accessible via help.salesforce.com or login to the applicable Service.

"**Free Services**" means Services that SFDC makes available to Customer free of charge. Free Services exclude Services offered as a free trial and Purchased Services.

"**Malicious Code**" means code, files, scripts, agents or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

"**Marketplace**" means an online directory, catalog or marketplace of applications that interoperate with the Services, including, for example, the AppExchange at http://www.salesforce.com/appexchange, Mulesoft Anypoint Exchange at https://www.mulesoft.com/exchange, or the Heroku Elements Marketplace at https://elements.heroku.com/, and any successor websites.

"**Non-SFDC Application**" means Web-based, mobile, offline or other software functionality that interoperates with a Service, that is provided by Customer or a third party and/or listed on a Marketplace including as Salesforce Labs or under similar designation. Non-SFDC Applications, other than those obtained or provided by Customer, will be identifiable as such.

"**Order Form**" means an ordering document or online order specifying the Services to be provided hereunder that is entered into between Customer and SFDC or any of their Affiliates, including any addenda and supplements thereto. By entering into an Order Form hereunder, an Affiliate agrees to be bound by the terms of this Agreement as if it were an original party hereto.

"**Purchased Services**" means Services that Customer or Customer's Affiliate purchases under an Order Form or online purchasing portal, as distinguished from Free Services or those provided pursuant to a free trial.

"**Services**" means the products and services that are ordered by Customer under an Order Form or online purchasing portal, or provided to Customer free of charge (as applicable) or under a free trial, and made available online by SFDC, including associated SFDC offline or mobile components, as described in the Documentation. "Services" exclude Content and Non-SFDC Applications.

"**SFDC**" means the Salesforce company described in the "SFDC Contracting Entity, Notices, Governing Law, and Venue" section below.

"**User**" means, in the case of an individual accepting these terms on his or her own behalf, such individual, or, in the case of an individual accepting this Agreement on behalf of a company or other legal entity, an individual who is authorized by Customer to use a Service, for whom Customer has purchased a subscription (or in the case of any Services provided by SFDC without charge, for whom a Service has been provisioned), and to whom Customer (or, when applicable, SFDC at Customer's request) has supplied a user identification and password (for Services utilizing authentication). Users may include, for example, employees, consultants, contractors and agents of Customer, and third parties with which Customer transacts business.

2. SFDC RESPONSIBILITIES

2.1 Provision of Purchased Services. SFDC will (a) make the Services and Content available to Customer pursuant to this Agreement, and the applicable Order Forms and Documentation, (b) provide applicable SFDC standard support for the Purchased Services to Customer at no additional charge, and/or upgraded support if purchased, (c) use commercially reasonable efforts to make the online Purchased Services available 24 hours a day, 7 days a week, except for: (i) planned downtime (of which SFDC shall give advance electronic notice), and (ii) any unavailability caused by circumstances beyond SFDC's reasonable control, including, for example, an act of God, act of government, flood, fire, earthquake, civil unrest, act of terror, strike or other labor problem (other than one involving SFDC employees), Internet service provider failure or delay, Non-SFDC Application, or denial of service attack, and (d) provide the Services in accordance with laws and government regulations applicable to SFDC's provision of its Services to its customers generally (i.e., without regard for Customer's particular use of the Services), and subject to Customer's and Users' use of the Services in accordance with this Agreement, the Documentation and the applicable Order Form.

2.2 Protection of Customer Data. SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users). The terms of the data processing addendum at https://www.salesforce.com/company/legal/agreements/ ("DPA") posted as of the Effective Date are hereby incorporated by reference. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by SFDC, its Processor Binding Corporate Rules,, and/or the Standard Contractual Clauses shall apply, as further set forth in the DPA. For the purposes of the Standard Contractual Clauses, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and an applicable Affiliate's execution of an Order Form, shall be treated as its execution of the Standard

Contractual Clauses and Appendices. Upon request by Customer made within 30 days after the effective date of termination or expiration of this Agreement, SFDC will make Customer Data available to Customer for export or download as provided in the Documentation. After such 30-day period, SFDC will have no obligation to maintain

or provide any Customer Data, and as provided in the Documentation will thereafter delete or destroy all copies of Customer Data in its systems or otherwise in its possession or control, unless legally prohibited.

2.3 SFDC Personnel. SFDC will be responsible for the performance of its personnel (including its employees and contractors) and their compliance with SFDC's obligations under this Agreement, except as otherwise specified in this Agreement.

2.4 Beta Services. From time to time, SFDC may make Beta Services available to Customer at no charge. Customer may choose to try such Beta Services or not in its sole discretion. Any use of Beta Services is subject to the Beta Services terms at https://www.salesforce.com/company/legal/agreements/.

2.5 Free Trial. If Customer registers on SFDC's or an Affiliate's website for a free trial, SFDC will make the applicable Service(s) available to Customer on a trial basis free of charge until the earlier of (a) the end of the free trial period for which Customer registered to use the applicable Service(s), or (b) the start date of any Purchased Service subscriptions ordered by Customer for such Service(s), or (c) termination by SFDC in its sole discretion. Additional trial terms and conditions may appear on the trial registration web page. Any such additional terms and conditions are incorporated into this Agreement by reference and are legally binding.

ANY DATA CUSTOMER ENTERS INTO THE SERVICES, AND ANY CUSTOMIZATIONS MADE TO THE SERVICES BY OR FOR CUSTOMER, DURING CUSTOMER'S FREE TRIAL WILL BE PERMANENTLY LOST UNLESS CUSTOMER PURCHASES A SUBSCRIPTION TO THE SAME SERVICES AS THOSE COVERED BY THE TRIAL, PURCHASES APPLICABLE UPGRADED SERVICES, OR EXPORTS SUCH DATA, BEFORE THE END OF THE TRIAL PERIOD. CUSTOMER CANNOT TRANSFER DATA ENTERED OR CUSTOMIZATIONS MADE DURING THE FREE TRIAL TO A SERVICE THAT WOULD BE A DOWNGRADE FROM THAT COVERED BY THE TRIAL (E.G., FROM ENTERPRISE EDITION TO PROFESSIONAL EDITION); THEREFORE, IF CUSTOMER PURCHASES A SERVICE THAT WOULD BE A DOWNGRADE FROM THAT COVERED BY THE TRIAL, CUSTOMER MUST EXPORT CUSTOMER DATA BEFORE THE END OF THE TRIAL PERIOD OR CUSTOMER DATA WILL BE PERMANENTLY LOST.

NOTWITHSTANDING THE "REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS" SECTION AND "INDEMNIFICATION BY SFDC" SECTION BELOW, DURING THE FREE TRIAL THE SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY AND SFDC SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE SERVICES FOR THE FREE TRIAL PERIOD UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE SFDC'S LIABILITY WITH RESPECT TO THE SERVICES PROVIDED DURING THE FREE TRIAL SHALL NOT EXCEED $1,000.00. WITHOUT LIMITING THE FOREGOING, SFDC AND ITS AFFILIATES AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO CUSTOMER THAT: (A) CUSTOMER'S USE OF THE SERVICES DURING THE FREE TRIAL PERIOD WILL MEET CUSTOMER'S REQUIREMENTS, (B) CUSTOMER'S USE OF THE SERVICES DURING THE FREE TRIAL PERIOD WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR, AND (C) USAGE DATA PROVIDED DURING THE FREE TRIAL PERIOD WILL BE ACCURATE. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE "LIMITATION OF LIABILITY" SECTION BELOW, CUSTOMER SHALL BE FULLY LIABLE UNDER THIS AGREEMENT TO SFDC AND ITS AFFILIATES FOR ANY DAMAGES ARISING OUT OF CUSTOMER'S USE OF THE SERVICES DURING THE FREE TRIAL PERIOD, ANY BREACH BY CUSTOMER OF THIS AGREEMENT AND ANY OF CUSTOMER'S INDEMNIFICATION OBLIGATIONS HEREUNDER.

CUSTOMER SHALL REVIEW THE APPLICABLE SERVICE'S DOCUMENTATION DURING THE TRIAL PERIOD TO BECOME FAMILIAR WITH THE FEATURES AND FUNCTIONS OF THE SERVICES BEFORE MAKING A PURCHASE.

2.6 Free Services. SFDC may make Free Services available to Customer. Use of Free Services is subject to the terms and conditions of this Agreement. In the event of a conflict between this section and any other portion of this Agreement, this section shall control. Free Services are provided to Customer without charge up to certain limits as described in the Documentation. Usage over these limits requires Customer's purchase of additional resources or services. Customer agrees that SFDC, in its sole discretion and for any or no reason, may terminate Customer's access to the Free Services or any part thereof. Customer agrees that any termination of Customer's access to the Free Services may be without prior notice, and Customer agrees that SFDC will not be liable to Customer or any third party for such termination. Customer is solely responsible for exporting Customer

Data from the Free Services prior to termination of Customer's access to the Free Services for any reason, provided that if SFDC terminates Customer's account, except as required by law SFDC will provide Customer a reasonable opportunity to retrieve its Customer Data.

NOTWITHSTANDING THE "REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS" SECTION AND "INDEMNIFICATION BY SFDC" SECTION BELOW, THE FREE SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY AND SFDC SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE FREE SERVICES UNLESS SUCH EXCLUSION OF LIABILITY IS NOT ENFORCEABLE UNDER APPLICABLE LAW IN WHICH CASE SFDC'S LIABILITY WITH RESPECT TO THE FREE SERVICES SHALL NOT EXCEED $1,000.00. WITHOUT LIMITING THE FOREGOING, SFDC AND ITS AFFILIATES AND ITS LICENSORS DO NOT REPRESENT OR WARRANT TO CUSTOMER THAT: (A) CUSTOMER'S USE OF THE FREE SERVICES WILL MEET CUSTOMER'S REQUIREMENTS, (B) CUSTOMER'S USE OF THE FREE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR, AND (C) USAGE DATA PROVIDED THROUGH THE FREE SERVICES WILL BE ACCURATE. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THE "LIMITATION OF LIABILITY" SECTION BELOW, CUSTOMER SHALL BE FULLY LIABLE UNDER THIS AGREEMENT TO SFDC AND ITS AFFILIATES FOR ANY DAMAGES ARISING OUT OF CUSTOMER'S USE OF THE FREE SERVICES, ANY BREACH BY CUSTOMER OF THIS AGREEMENT AND ANY OF CUSTOMER'S INDEMNIFICATION OBLIGATIONS HEREUNDER.

3. USE OF SERVICES AND CONTENT

3.1 Subscriptions. Unless otherwise provided in the applicable Order Form or Documentation, (a) Purchased Services and access to Content are purchased as subscriptions for the term stated in the applicable Order Form or in the applicable online purchasing portal, (b) subscriptions for Purchased Services may be added during a subscription term at the same pricing as the underlying subscription pricing, prorated for the portion of that subscription term remaining at the time the subscriptions are added, and (c) any added subscriptions will terminate on the same date as the underlying subscriptions. Customer agrees that its purchases are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by SFDC regarding future functionality or features.

3.2 Usage Limits. Services and Content are subject to usage limits specified in Order Forms and Documentation. If Customer exceeds a contractual usage limit, SFDC may work with Customer to seek to reduce Customer's usage so that it conforms to that limit. If, notwithstanding SFDC's efforts, Customer is unable or unwilling to abide by a contractual usage limit, Customer will execute an Order Form for additional quantities of the applicable Services or Content promptly upon SFDC's request, and/or pay any invoice for excess usage in accordance with the "Invoicing and Payment" section below.

3.3 Customer Responsibilities. Customer will (a) be responsible for Users' compliance with this Agreement, Documentation and Order Forms, (b) be responsible for the accuracy, quality and legality of Customer Data, the means by which Customer acquired Customer Data, Customer's use of Customer Data with the Services, and the interoperation of any Non-SFDC Applications with which Customer uses Services or Content, (c) use commercially reasonable efforts to prevent unauthorized access to or use of Services and Content, and notify SFDC promptly of any such unauthorized access or use, (d) use Services and Content only in accordance with this Agreement, Documentation, the Acceptable Use and External Facing Services Policy and the Artificial Intelligence Acceptable Use Policy both available at https://www.salesforce.com/company/legal/agreements/, Order Forms and applicable laws and government regulations, and (e) comply with terms of service of any Non-SFDC Applications with which Customer uses Services or Content. Any use of the Services in breach of the foregoing by Customer or Users that in SFDC's judgment threatens the security, integrity or availability of SFDC's services, may result in SFDC's immediate suspension of the Services, however SFDC will use commercially reasonable efforts under the circumstances to provide Customer with notice and an opportunity to remedy such violation or threat prior to any such suspension.

3.4 Usage Restrictions. Customer will not (a) make any Service or Content available to anyone other than Customer or Users, or use any Service or Content for the benefit of anyone other than Customer or its Affiliates, unless expressly stated otherwise in an Order Form or the Documentation, (b) sell, resell, license, sublicense, distribute, rent or lease any Service or Content, or include any Service or Content in a service bureau or outsourcing offering, (c) use a Service or Non-SFDC Application to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use a Service or Non-SFDC Application to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of any Service or third-party data contained therein, (f) attempt to gain unauthorized access

to any Service or Content or its related systems or networks, (g) permit direct or indirect access to or use of any Services or Content in a way that circumvents a contractual usage limit, or use any Services to access, copy or use any of SFDC intellectual property except as permitted under this Agreement, an Order Form, or the Documentation, (h) modify, copy, or create derivative works of a Service or any part, feature, function or user interface thereof, (i) copy Content except as permitted herein or in an Order Form or the Documentation, (j) frame or mirror any part of any Service or Content, other than framing on Customer's own intranets or otherwise for its own internal business purposes or as permitted in the Documentation, (k) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile a Service or Content or access it to (1)

build a competitive product or service, (2) build a product or service using similar ideas, features, functions or graphics of the Service, (3) copy any ideas, features, functions or graphics of the Service, or (4) determine whether the Services are within the scope of any patent.

3.5 Removal of Content and Non-SFDC Applications. If Customer receives notice, including from SFDC, that Content or a Non-SFDC Application may no longer be used or must be removed, modified and/or disabled to avoid violating applicable law, third-party rights, or the Acceptable Use and External Facing Services Policy, Customer will promptly do so. If Customer does not take required action, including deleting any Content Customer may have downloaded from the Services, in accordance with the above, or if in SFDC's judgment continued violation is likely to reoccur, SFDC may disable the applicable Content, Service and/or Non-SFDC Application. If requested by SFDC, Customer shall confirm deletion and discontinuance of use of such Content and/or Non-SFDC Application in writing and SFDC shall be authorized to provide a copy of such confirmation to any such third-party claimant or governmental authority, as applicable. In addition, if SFDC is required by any third-party rights holder to remove Content, or receives information that Content provided to Customer may violate applicable law or third-party rights, SFDC may discontinue Customer's access to Content through the Services.

4. NON-SFDC PRODUCTS AND SERVICES

4.1 Non-SFDC Products and Services. SFDC or third parties may make available (for example, through a Marketplace or otherwise) third-party products or services, including, for example, Non-SFDC Applications and implementation and other consulting services. Any acquisition by Customer of such products or services, and any exchange of data between Customer and any Non-SFDC provider, product or service is solely between Customer and the applicable Non-SFDC provider. SFDC does not warrant or support Non-SFDC Applications or other Non-SFDC products or services, whether or not they are designated by SFDC as "certified" or otherwise, unless expressly provided otherwise in an Order Form. SFDC is not responsible for any disclosure, modification or deletion of Customer Data resulting from access by such Non-SFDC Application or its provider.

4.2 Integration with Non-SFDC Applications. The Services may contain features designed to interoperate with Non-SFDC Applications. SFDC cannot guarantee the continued availability of such Service features, and may cease providing them without entitling Customer to any refund, credit, or other compensation, if for example and without limitation, the provider of a Non-SFDC Application ceases to make the Non-SFDC Application available for interoperation with the corresponding Service features in a manner acceptable to SFDC.

5. FEES AND PAYMENT

5.1 Fees. Customer will pay all fees specified in Order Forms. Except as otherwise specified herein or in an Order Form, (i) fees are based on Services and Content subscriptions purchased and not actual usage, (ii) payment obligations are non- cancelable and fees paid are non-refundable, and (iii) quantities purchased cannot be decreased during the relevant subscription term.

5.2 Invoicing and Payment. Customer will provide SFDC with valid and updated credit card information, or with a valid purchase order or alternative document reasonably acceptable to SFDC. If Customer provides credit card information to SFDC, Customer authorizes SFDC to charge such credit card for all Purchased Services listed in the Order Form for the initial subscription term and any renewal subscription term(s) as set forth in the "Term of Purchased Subscriptions" section below. Such charges shall be made in advance, either annually or in accordance with any different billing frequency stated in the applicable Order Form. If the Order Form specifies that payment will be by a method other than a credit card, SFDC will invoice Customer in advance and otherwise in accordance with the relevant Order Form. Unless otherwise stated in the Order Form, invoiced fees are due net 30 days from the invoice date. Customer is responsible for providing complete and accurate billing and contact information to SFDC and notifying SFDC of any changes to such information.

5.3 Overdue Charges. If any invoiced amount is not received by SFDC by the due date, then without limiting SFDC's rights or remedies, (a) those charges may accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, and/or (b) SFDC may condition future subscription renewals and Order Forms on

payment terms shorter than those specified in the "Invoicing and Payment" section above.

5.4 Suspension of Service and Acceleration. If any charge owing by Customer under this or any other agreement for services is 30 days or more overdue, (or 10 or more days overdue in the case of amounts Customer has authorized SFDC to charge to Customer's credit card), SFDC may, without limiting its other rights and remedies, accelerate Customer's unpaid fee obligations under such agreements so that all such obligations become immediately due and payable, and suspend Services until such amounts are paid in full, provided that, other than for customers paying by credit card or direct debit whose payment has been declined, SFDC will give Customer at least 10 days' prior notice that its account is overdue, in accordance with the "Manner of Giving Notice" section below for billing notices, before suspending services to Customer.

5.5 Payment Disputes. SFDC will not exercise its rights under the "Overdue Charges" or "Suspension of Service and Acceleration" section above if Customer is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

5.6 Taxes. SFDC's fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction whatsoever (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If SFDC has the legal obligation to pay or collect Taxes for which Customer is responsible under this section, SFDC will invoice Customer and Customer will pay that amount unless Customer provides SFDC with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, SFDC is solely responsible for taxes assessable against it based on its income, property and employees.

6. PROPRIETARY RIGHTS AND LICENSES

6.1 Reservation of Rights. Subject to the limited rights expressly granted hereunder, SFDC, its Affiliates, its licensors and Content Providers reserve all of their right, title and interest in and to the Services and Content, including all of their related intellectual property rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

6.2 Access to and Use of Content. Customer has the right to access and use applicable Content subject to the terms of applicable Order Forms, this Agreement and the Documentation.

6.3 License by Customer to SFDC. Customer grants SFDC, its Affiliates and applicable contractors a worldwide, limited-term license to host, copy, use, transmit, and display any Non-SFDC Applications and program code created by or for Customer using a Service or for use by Customer with the Services, and Customer Data, each as appropriate for SFDC to provide and ensure proper operation of the Services and associated systems in accordance with this Agreement. If Customer chooses to use a Non-SFDC Application with a Service, Customer grants SFDC permission to allow the Non-SFDC Application and its provider to access Customer Data and information about Customer's usage of the Non-SFDC Application as appropriate for the interoperation of that Non-SFDC Application with the Service. Subject to the limited licenses granted herein, SFDC acquires no right, title or interest from Customer or its licensors under this Agreement in or to any Customer Data, Non-SFDC Application or such program code.

6.4 License by Customer to Use Feedback. Customer grants to SFDC and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use, distribute, disclose, and make and incorporate into its services any suggestion, enhancement request, recommendation, correction or other feedback provided by Customer or Users relating to the operation of SFDC's or its Affiliates' services.

6.5 Federal Government End Use Provisions. SFDC provides the Services, including related software and technology, for ultimate federal government end use in accordance with the following: The Services consist of "commercial items," as defined at FAR 2.101. In accordance with FAR 12.211-12.212 and DFARS 227.7102-4 and 227.7202-4, as applicable, the rights of the U.S. Government to use, modify, reproduce, release, perform, display, or disclose commercial computer software, commercial computer software documentation, and technical data furnished in connection with the Services shall be as provided in this Agreement, except that, for U.S. Department of Defense end users, technical data customarily provided to the public is furnished in accordance with DFARS 252.227-7015. If a government agency needs additional rights, it must negotiate a mutually acceptable written addendum to this Agreement specifically granting those rights.

7. CONFIDENTIALITY

7.1 Definition of Confidential Information. "Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential

Information of Customer includes Customer Data; Confidential Information of SFDC includes the Services and Content, and the terms and conditions of this Agreement and all Order Forms (including pricing). Confidential Information of each party includes business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without knowledge of any breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party. For the avoidance of doubt, the non-disclosure obligations set forth in this "Confidentiality" section apply to Confidential Information exchanged between the parties in connection with the evaluation of additional SFDC services.

7.2 Protection of Confidential Information. As between the parties, each party retains all ownership rights in and to its Confidential Information. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care) to (i) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those herein. Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel and accountants without the other party's prior written consent, provided that a party that makes any such disclosure to its Affiliate, legal counsel or accountants will remain responsible for such Affiliate's, legal counsel's or accountant's compliance with this "Confidentiality" section. Notwithstanding the foregoing, SFDC may disclose the terms of this Agreement and any applicable Order Form to a contractor or Non-SFDC Application Provider to the extent necessary to perform SFDC's obligations under this Agreement, under terms of confidentiality materially as protective as set forth herein.

7.3 Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information.

8. REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS 8.1 Representations.

Each party represents that it has validly entered into this Agreement and has the legal power to do so.

8.2 SFDC Warranties. SFDC warrants that during an applicable subscription term (a) this Agreement, the Order Forms and the Documentation will accurately describe the applicable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, (b) SFDC will not materially decrease the overall security of the Services, (c) the Services will perform materially in accordance with the applicable Documentation, and (d) subject to the "Integration with Non-SFDC Applications" section above, SFDC will not materially decrease the overall functionality of the Services. For any breach of a warranty above, Customer's exclusive remedies are those described in the "Termination" and "Refund or Payment upon Termination" sections below.

8.3 Disclaimers. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. SERVICES PROVIDED FREE OF CHARGE, CONTENT AND BETA SERVICES ARE PROVIDED "AS IS," AND AS AVAILABLE EXCLUSIVE OF ANY WARRANTY WHATSOEVER.

9. MUTUAL INDEMNIFICATION

9.1 Indemnification by SFDC. SFDC will defend Customer against any claim, demand, suit or proceeding made or brought against Customer by a third party alleging that any Purchased Service infringes or misappropriates such third party's intellectual

property rights (a "Claim Against **Customer**"), and will indemnify Customer from any damages, attorney fees and costs finally awarded against Customer as a result of, or for amounts paid by Customer under a settlement approved by SFDC in writing of, a Claim Against Customer, provided Customer (a) promptly gives SFDC written notice of the Claim Against Customer, (b) gives SFDC sole control of the defense and settlement of the Claim Against Customer (except that SFDC may not settle any Claim Against Customer unless it unconditionally releases Customer of all liability), and (c) gives SFDC all reasonable assistance, at SFDC's expense. If SFDC receives information about an infringement or misappropriation claim related to a Service, SFDC may in its discretion and at no cost to Customer (i) modify the Services so that they are no longer claimed to infringe or misappropriate, without breaching SFDC's warranties under "SFDC Warranties" above, (ii) obtain a license for Customer's continued use of that Service in accordance with this Agreement, or (iii) terminate Customer's subscriptions for that Service upon 30 days' written notice and refund Customer any prepaid fees covering the remainder of the term of the terminated subscriptions. The above defense and indemnification obligations do not apply if (I) the allegation does not state with specificity that the Services are the basis of the Claim Against Customer; (II) a Claim Against Customer arises from the use or combination of the Services or any part thereof with software, hardware, data, or processes not provided by SFDC, if the Services or use thereof would not infringe without such combination; (III) a Claim Against Customer arises from Services

under an Order Form for which there is no charge; or (IV) a Claim against Customer arises from Content, a Non-SFDC Application or Customer's breach of this Agreement, the Documentation or applicable Order Forms.

9.2 Indemnification by Customer. Customer will defend SFDC and its Affiliates against any claim, demand, suit or proceeding made or brought against SFDC by a third party (a) alleging that the combination of a Non-SFDC Application or configuration provided by Customer and used with the Services, infringes or misappropriates such third party's intellectual property rights, or (b) arising from (i) Customer's use of the Services or Content in an unlawful manner or in violation of the Agreement, the Documentation, or Order Form, (ii) any Customer Data or Customer's use of Customer Data with the Services, or (iii) a Non-SFDC Application provided by Customer(each a "Claim Against **SFDC**"), and will indemnify SFDC from any damages, attorney fees and costs finally awarded against SFDC as a result of, or for any amounts paid by SFDC under a settlement approved by Customer in writing of, a Claim Against SFDC, provided SFDC (A) promptly gives Customer written notice of the Claim Against SFDC, (B) gives Customer sole control of the defense and settlement of the Claim Against SFDC (except that Customer may not settle any Claim Against SFDC unless it unconditionally releases SFDC of all liability), and (C) gives Customer all reasonable assistance, at Customer's expense. The above defense and indemnification obligations do not apply if a Claim Against SFDC arises from SFDC's breach of this Agreement, the Documentation or applicable Order Forms.

9.3 Exclusive Remedy. This "Mutual Indemnification" section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any third-party claim described in this section.

10. LIMITATION OF LIABILITY

10.1 Limitation of Liability. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HEREUNDER FOR THE SERVICES GIVING RISE TO THE LIABILITY IN THE TWELVE MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER'S AND ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER THE "FEES AND PAYMENT" SECTION ABOVE.

10.2 Exclusion of Consequential and Related Damages. IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

11. TERM AND TERMINATION

11.1 Term of Agreement. This Agreement commences on the date Customer first accepts it and continues until all subscriptions hereunder have expired or have been terminated.

11.2 Term of Purchased Subscriptions. The term of each subscription shall be as specified in the applicable Order Form. Except as

otherwise specified in an Order Form, subscriptions will automatically renew for additional one year terms, unless either party gives the other written notice (email acceptable) at least 30 days before the end of the relevant subscription term. Except as expressly provided in the applicable Order Form, renewal of promotional or one-time priced subscriptions will be at SFDC's applicable list price in effect at the time of the applicable renewal. Notwithstanding anything to the contrary, any renewal in which subscription volume or subscription length for any Services has decreased from the prior term will result in re-pricing at renewal without regard to the prior term's per-unit pricing.

11.3 Termination. A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

11.4 Refund or Payment upon Termination. If this Agreement is terminated by Customer in accordance with the "Termination" section above, SFDC will refund Customer any prepaid fees covering the remainder of the term of all Order Forms after the effective date of termination. If this Agreement is terminated by SFDC in accordance with the "Termination" section above, Customer will pay any unpaid fees covering the remainder of the term of all Order Forms to the extent permitted by applicable law. In no event will termination relieve Customer of its obligation to pay any fees payable to SFDC for the period prior to the effective date of termination.

11.5 Surviving Provisions. The sections titled "Free Services," "Fees and Payment," "Proprietary Rights and Licenses," "Confidentiality," "Disclaimers," "Mutual Indemnification," "Limitation of Liability," "Refund or Payment upon Termination," "Removal of Content and Non-SFDC Applications," "Surviving Provisions" and "General Provisions" will survive any termination or expiration of this Agreement, and the section titled "Protection of Customer Data" will survive any termination or expiration of this Agreement for so long as SFDC retains possession of Customer Data.

12. GENERAL PROVISIONS

12.1 Export Compliance. The Services, Content, other SFDC technology, and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. SFDC and Customer each represents that it is not on any U.S. government denied-party list. Customer will not permit any User to access or use any Service or Content in a U.S.-embargoed country or region (currently the Crimea, Luhansk or Donetsk regions, Cuba, Iran, North Korea, or Syria) or as may be updated from time to time at https://www.salesforce.com/company/legal/compliance/ or in violation of any U.S. export law or regulation.

12.2 Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction.

12.3 Entire Agreement and Order of Precedence. This Agreement is the entire agreement between SFDC and Customer regarding Customer's use of Services and Content and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. The parties agree that any term or condition stated in a Customer purchase order or in any other Customer order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form, (2) this Agreement, and (3) the Documentation. Titles and headings of sections of this Agreement are for convenience only and shall not affect the construction of any provision of this Agreement.

12.4 Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. Each party will be solely responsible for payment of all compensation owed to its employees, as well as all employment-related taxes.

12.5 Third-Party Beneficiaries. There are no third-party beneficiaries under this Agreement.

12.6 Waiver. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right.

12.7 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

12.8 Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld); provided, however, either party may assign this Agreement in its entirety (including all Order Forms), without the other party's consent to its Affiliate or in connection with

a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. Notwithstanding the foregoing, if a party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favor of, a direct competitor of the other party, then such other party may terminate this Agreement upon written notice. In the event of such a termination, SFDC will refund Customer any prepaid fees covering the remainder of the term of all subscriptions for the period after the effective date of such termination. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

12.9 SFDC Contracting Entity, Notices, Governing Law, and Venue. The SFDC entity entering into this Agreement, the address to which Customer should direct notices under this Agreement, the law that will apply in any dispute or lawsuit arising out of or in connection with this Agreement, and the courts that have jurisdiction over any such dispute or lawsuit, depend on where Customer is domiciled.

For Customers domiciled in North or South America

If Customer is domiciled in:	The SFDC entity entering into this Agreement is:	Notices should be addressed to:	Governing law is:	Courts with exclusive jurisdiction are:
Any country other than Brazil or Canada	salesforce.com, inc.), a Delaware corporation	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, California, 94105, U.S.A., attn: VP, Worldwide Sales Operations, with a copy to attn: General Counsel	California and controlling United States federal law	San Francisco, California, U.S.A.
Salesforce, Inc. (f/k/a Brazil	Brazil Salesforce Tecnologia Ltda.	Av. Jornalista Roberto Marinho, 85, 14º Andar - Cidade Monções, CEP 04576-010 São Paulo - SP	Brazil	São Paulo, SP, Brazil
Canada	Canada salesforce.com Canada Corporation, a Nova Scotia corporation	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, California, 94105, U.S.A., attn: VP, Worldwide Sales Operations, with a copy to attn: General Counsel	Ontario and controlling Canadian federal law	Toronto, Ontario, Canada

For Customers domiciled in Europe, the Middle East, or Africa

If Customer is domiciled in:	The SFDC entity entering into this Agreement is:	Notices should be addressed to:	Governing law is:	Courts with exclusive jurisdiction are:
Any country other than France, Germany, Italy, Spain, or the United Kingdom	SFDC Ireland Limited, a limited liability company incorporated in Ireland	26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom, attn: VP, Sales Operations, with a copy to attn.: Legal Department - Salesforce Tower, 60 R801, North Dock, Dublin, Ireland	England	England London, England
	Salesforce UK Limited,			

		limited liability company, incorporated in Germany	Sales Operations, with a copy to attn.: Legal Department - Erika-Mann-Strasse 31-37, 80636 München, Germany
France salesforce.com France, a French S.A.S company with a share capital of 37,000 €, registered with the Paris Trade Registry under number 483 993 226 RCS Paris, Registered office: 3 Avenue Octave Gréard, 75007 Paris, France	Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom, attn: VP, Sales Operations, with a copy to attn.: Legal Department - Service Juridique, 3 Avenue Octave Gréard, 75007 Paris, France		France Paris, France
Germany salesforce.com Germany GmbH, a	Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom, attn: VP,		Germany Munich, Germany

Italy salesforce.com Italy S.r.l., an Italian limited liability company having its registered address at Piazza Filippo Meda 5, 20121 Milan (MI), VAT / Fiscal code n. 04959160963			Italy Milan, Italy Spain Madrid,
Spain Salesforce Systems Spain, S.L., a limited liability company incorporated in Spain	Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom, attn: VP, Sales Operations, with a copy to attn.: Legal Department - Paseo de la Castellana 79, Madrid, 28046, Spain		Spain
United Kingdom Salesforce UK Limited, a limited liability company incorporated in England	Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom, attn: VP, Sales	Operations, with a copy to attn: Legal Department, Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N	4AY, United Kingdom England London, England

For Customers domiciled in Asia or the Pacific Region

If Customer is domiciled in:	The SFDC entity entering into this Agreement is:	Notices should be addressed to:	Governing law is:	Courts with exclusive jurisdiction are:
Any country other than Australia, India, Japan, or New Zealand	salesforce.com Singapore Pte Ltd, a Singapore private limited company	5 Temasek Boulevard #13-01, Suntec Tower 5, Singapore, 038985, attn: Director, APAC Sales Operations, with a copy to attn: General Counsel	Singapore	Singapore
Australia or New Zealand	SFDC Australia Pty Ltd	Salesforce Tower, Level 39, 180 George St, Sydney NSW 2000, attn: Senior Director, Finance with a copy to attn: General Counsel	New South Wales, Australia	New South Wales, Australia
India	Salesforce.com India Private Limited, a company incorporated under the provisions of the Companies Act, 1956 of India	Torrey Pines, 3rd Floor, Embassy Golflinks Software Business Park Bengaluru, Karnataka 560071, India	India	India Bengaluru , India
Japan	Salesforce Japan Co., Ltd. (f/k/a Kabushiki Kaisha Salesforce.com), a Japan corporation	1-1-3, Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan, attn: Senior Director, Japan Sales Operations, with a copy to attn: General Counsel	Japan	Japan Tokyo,
	Salesforce.com India Private Limited			

12.10 Manner of Giving Notice. Except as otherwise specified in this Agreement, all notices related to this Agreement will be in writing and will be effective upon (a) personal delivery, (b) the second business day after mailing, or (c), except for notices of termination or an indemnifiable claim ("Legal Notices"), which shall clearly be identifiable as Legal Notices, the day of sending by email. Billing-related notices to Customer will be addressed to the relevant billing contact designated by Customer. All other notices to Customer will be addressed to the relevant Services system administrator designated by Customer.

12.11 Agreement to Governing Law and Jurisdiction. Each party agrees to the applicable governing law above without regard to choice or conflicts of law rules, and to the exclusive jurisdiction of the applicable courts above.

12.12 Local Law Requirements: France.

With respect to Customers domiciled in France, the following provisions shall be applicable :

(1) Section 8.2 "SFDC Warranties" is replaced by the following :

8.2 SFDC Warranties. During an applicable subscription term (a) this Agreement, the Order Forms and the Documentation will accurately describe the applicable administrative, physical, and technical safeguards for

protection of the security, confidentiality and integrity of Customer Data, (b) SFDC will not materially decrease the overall security of the Services, (c) the Services will perform materially in accordance with the applicable Documentation, and (d) subject to the "Integration with Non-SFDC Applications" section above, SFDC will not materially decrease the overall functionality of the Services.

(2) a new Section 12.12.1 is added as follows:

12.12.1 PGSSI-S. To the extent Customer is subject to Article L.1111-8 (or any successor thereto) of the French public health code (Code de la Santé Publique), Customer shall abide by the Global Information Security Policy for the Healthcare Sector (PGSSI-S) pursuant to Article L.1110-4-1 (or any successor thereto) of the aforementioned code.

(3) a new Section 12.12.2 is added as follows :

12.12.2 Exclusions. To the extent permitted under applicable law, the provisions of Article 1222 and 1223 of the French Civil Code shall in no event be applicable.

(4) a new Section 12.12.3 is added as follows :

12.12.3 Language. The Parties agree that this Agreement and/or any Documentation and other information or policies referenced or attached to this Agreement may be in English.

(5) a new Section 12.12.4 is added as follows :

12.12.4 Independence Towards Third Parties. For the avoidance of doubt, any third parties, including those Customer contracted with to provide consulting and/or implementation services in relation to the Services, are independent of SFDC and SFDC shall in no event be responsible for their acts or omissions, including when such acts or omissions impact Customer's use of the Services.

(6) in the event of any conflict between any statutory law in France applicable to Customer, and the terms and conditions of this Agreement, the applicable statutory law shall prevail.

12.13 Local Law Requirements: Germany. With respect to Customers domiciled in Germany, Section 8 "REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS", Section 9.3 "Exclusive Remedy", and Section 10 "LIMITATION OF LIABILITY" of this Agreement are replaced with the following sections respectively:

8 WARRANTIES FOR CUSTOMERS DOMICILED IN GERMANY

8.1 Agreed Quality of the Services. SFDC warrants that during an applicable subscription term (a) this Agreement, the Order Forms and the Documentation will accurately describe the applicable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, (b) SFDC will not materially decrease the overall security of the Services, (c) the Services will perform materially in accordance with the applicable Documentation, and (d) subject to the "Integration with Non-SFDC Applications" section above, SFDC will not materially decrease the overall functionality of the Services.

8.2 Content. SFDC is not designating or adopting Content as its own and assumes no warranty or liability for Content. The parties agree that the "Reporting of Defects", "Remedies resulting from Defects" and "Exclusions" section shall apply accordingly to SFDC's responsibility in the event SFDC is deemed responsible for Content by a court of competent jurisdiction.

8.3 Reporting of Defects. Customer shall report any deviation of the Services from the "Agreed Quality of the Services" section ("Defect") to SFDC in writing without undue delay and shall submit a detailed description of the Defect or, if not possible, of the symptoms of the Defect. Customer shall forward to SFDC any useful information available to Customer for rectification of the Defect.

8.4 Remedies Resulting from Defects. SFDC shall rectify any Defect within a reasonable period of time. If such rectification fails, Customer may terminate the respective Order Form provided that SFDC had enough time for curing the Defect. In the "Refund or Payment upon Termination" section, sentence 1 and sentence 3 shall apply accordingly. If SFDC is responsible for the Defect or if SFDC is in default with the rectification, Customer may assert claims for the damage caused in the scope specified in the "Limitation of Liability" section below.

8.5 Defects in Title. Defects in title of the Services shall be handled in accordance with the provisions of Clause 9 "Mutual Indemnification".

8.6 Exclusions. Customer shall have no claims under this Clause 8 "Warranty" if a Defect was caused by the Services not being used by Customer in accordance with the provisions of this Agreement, the Documentation and the applicable Order Forms.

9.3 Liability resulting from Indemnification for Customers domiciled in Germany. The below "Limitation of Liability" section shall apply to any claims resulting from this "Mutual Indemnification" section.

10. LIMITATION OF LIABILITY FOR CUSTOMERS DOMICILED IN GERMANY

10.1 Unlimited Liability. The Parties shall be mutually liable without limitation
(a) in the event of willful misconduct or gross negligence,
(b) within the scope of a guarantee taken over by the respective party,
(c) in the event that a defect is maliciously concealed,
(d) in case of an injury to life, body or health,
(e) according to the German Product Liability Law.

10.2 Liability for Breach of Cardinal Duties. If cardinal duties are infringed due to slight negligence and if, as a consequence, the achievement of the objective of this Agreement including any applicable Order Form is endangered, or in the case of a slightly negligent failure to comply with duties, the very discharge of which is an essential prerequisite for the proper performance of this Agreement (including any applicable Order Form), the parties' liability shall be limited to foreseeable damage typical for the contract. In all other respects, any liability for damage caused by slight negligence shall be excluded.

10.3 Liability Cap. Unless the parties are liable in accordance with "Unlimited Liability" section above, in no event shall the aggregate liability of each party together with all of its Affiliates arising out of or related to this Agreement exceed the total amount paid by Customer and its Affiliates hereunder for the Services giving rise to the liability in the 12 months preceding the first incident out of which the liability arose. The foregoing limitation will not limit Customer's and its Affiliates' payment obligations under the "Fees and Payment" section above.

10.4 Scope. With the exception of liability in accordance with the "Unlimited Liability" section, the above limitations of liability shall apply to all claims for damages, irrespective of the legal basis including claims for tort damages. The above limitations of liability also apply in the case of claims for a party's damages against the respective other party's employees, agents or bodies.

12.14 Local Law Requirements: Italy. With respect to Customers domiciled in Italy, Section 5.2 "Invoicing and Payment", Section 5.3 "Overdue Charges," and Section 12.2 "Anti Corruption" of this Agreement are replaced with the following sections respectively:

5.2. Invoicing and Payment

5.2.1 Invoicing and Payment. Fees will be invoiced in advance and otherwise in accordance with the relevant Order Form. Unless otherwise stated in the Order Form, fees are due net 30 days from the invoice date. The parties acknowledge that invoices are also be submitted electronically by SFDC in accordance with the "Electronic Invoicing" section below through the Agenzia delle Entrate's Exchange System (SDI – Sistema di Interscambio) and any delay due to the SDI shall not affect the

foregoing payment term. Customer shall be responsible for providing complete and accurate billing and contact information to SFDC and shall notify SFDC of any changes to such information.

5.2.2 Electronic Invoicing. The invoice will be issued in electronic format as defined in article 1, paragraph 916, of Law no. 205 of December 27, 2017, which introduced the obligation of electronic invoicing, starting from January 1, 2019, for the sale of goods and services performed between residents, established or identified in the territory of the Italian State. To facilitate such electronic invoicing, Customer shall provide to SFDC at least the following information in writing: Customer full registered company name, registered office address, VAT number, tax/fiscal code and any additional code and/or relevant information required under applicable law. In any event, the parties shall cooperate diligently to enable such electronic invoicing process. Any error due to the provision by Customer of incorrect or insufficient invoicing information preventing (a) SFDC to successfully submit the electronic invoice to the SDI or (b) the SDI to duly and effectively process such invoice or (c) which, in

any event, requires SFDC to issue an invoice again, shall not result in an extension of the payment term set out in the "Invoicing and Payment" section above, and such term shall still be calculated from the date of the original invoice. SFDC reserves the right to provide any invoice copy in electronic form via email in addition to the electronic invoicing described herein.

5.2.3 Split Payment. If subject to the "split payment" regime, Customer shall be exclusively responsible for payment of any VAT amount due, provided that Customer shall confirm to SFDC the applicability of such regime and, if applicable, Customer shall provide proof of such VAT payment to SFDC and, if applicable, Customer shall provide proof of such VAT payment to SFDC.

5.3 Overdue Charges. Subject to the "Payment Disputes" section below, if any invoiced amount is not received by SFDC by the due date, then without limiting SFDC's rights or remedies, those charges, without the need for notice of default, may accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law (Legislative Decree no. 231/2002), whichever is lower and/or (b) SFDC may condition future subscription renewals and Order Forms on payment terms shorter than those specified in the "Invoicing and Payment" section above.

12.2 Anti-Corruption.

12.2.1 Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction.

12.2.2 Code of Conduct and Organization, Management and Control Model. Customer acknowledges that SFDC has adopted an Organization, Management and Control Model pursuant to Legislative Decree 231/2001 to prevent crimes provided for therein and commits to comply with the principles contained in the above Legislative Decree 231/2001 and in the SFDC Code of Conduct which is available at the following link: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/sfdc-code-of-conduct.pdf. Customer also acknowledges and agrees that the violation of the principles and the provisions contained in Legislative Decree 231/2001 and in the SFDC Code of Conduct by Customer may entitle SFDC, based on the severity of the violation, to terminate this Agreement for cause as set out in Section 11.3(i) above.

12.15 Local Law Requirements: Spain. With respect to Customers domiciled in Spain, in the event of any conflict between any statutory law in Spain applicable to Customer, and the terms and conditions of this Agreement, the applicable statutory law shall prevail.

12.16 Local Law Requirements: India. With respect to Customers domiciled in India, the following shall apply:

12.16.1 Venue and Arbitration

A. Subject to the "Arbitration" Section below, the courts located in Bengaluru , India shall have exclusive jurisdiction over any dispute relating to this Agreement, and each party hereby consents to the exclusive jurisdiction of such courts. Without prejudice to the generality of the foregoing, the courts at Bengaluru, India shall have exclusive jurisdiction on matters arising from, relating to, or in connection with an award made under the "Arbitration" Section below.

B. **Arbitration**. In the event of any dispute, controversy or claim between the Parties hereto arising out of or relating to this Agreement, the Parties shall first seek to resolve the dispute in good faith through informal discussion. If such dispute, controversy, or claim cannot be resolved informally within a period of 10 (ten) business days from the date on which the dispute arose, the Parties agree that it shall be settled by binding arbitration to be held before a panel consisting of 3 (three) arbitrators, where each Party shall appoint an arbitrator and such arbitrators shall appoint the third and presiding arbitrator.

The arbitration shall be conducted in accordance with provisions of the (Indian) Arbitration and Conciliation Act, 1996, as amended from time to time ("**Arbitration Act**"). The seat and venue of the arbitration shall be Bengaluru , India. The language of the arbitration shall be English. The Parties agree that any of them may seek interim measures under section 9 of the Arbitration Act, including injunctive relief in relation to the provisions of this Agreement or the Parties' performance of it from courts in Bengaluru, India, without prejudice to any other right the Parties may have under the Arbitration Act and other applicable laws. The arbitration panel's decision shall be final, conclusive and binding on the parties to the arbitration. The Parties shall each pay one-half of the costs and expenses of such arbitration, and each shall separately pay its respective counsel fees and expenses. The prevailing Party may, in the judgement of the arbitration panel, be entitled to recover its fees and expenses. All dispute resolution proceedings, all matters pertaining to such proceedings and all documents and

submissions made pursuant thereto shall be strictly confidential and subject to the provisions of "Confidentiality" Section of this Agreement.

12.16.2 Section 5.2 "Invoicing and Payment" of this Agreement is replaced with the following

section: **5.2 Invoicing and Payment**

5.2.1 Invoicing and Payment. Unless otherwise stated in the relevant Order Form, fees (i) will be invoiced in advance, and (ii) are due net 30 days from the invoice date.. The parties acknowledge that invoices are also to be submitted electronically by SFDC in accordance with the "Electronic Invoicing" section below through the Government of India's e-invoicing system ("GST Portal") and any delay due to such submission shall not affect the foregoing payment term. Customer shall be responsible for providing complete and accurate billing and contact information to SFDC and shall notify SFDC of any changes to such information.

5.2.2 Electronic Invoicing. Customer shall provide to SFDC at least the following information in writing to facilitate electronic invoicing: Customers full registered company/legal entity name, registered office address, goods and services tax identification number, address and/or relevant information required under applicable law. In any event, the parties shall cooperate diligently to enable such electronic invoicing process. Any error/delay in issuance of the electronic invoice due to: (a) the provision by Customer of incorrect or insufficient invoicing information preventing SFDC from successfully submitting the electronic invoice to the GST Portal; or (b) the GST Portal and/or any other government authority (or their designated agent/agency) not being able to duly and effectively process such invoice; or (c) any event which requires SFDC to issue an invoice again; shall not result in an extension of the payment term set out in the "Invoicing and Payment" section above, and such term shall still be calculated from the date of the original invoice. SFDC reserves the right to provide any invoice copy in electronic form via email in addition to the electronic invoicing described herein.

12.17 Local Law Requirements: United Kingdom. With respect to Customers domiciled in the United Kingdom, Section 12.3 "Entire Agreement and Order of Precedence" of this Agreement is replaced with the following section:

12.3 Entire Agreement and Order of Precedence. This Agreement is the entire agreement between SFDC and Customer regarding Customer's use of Services and Content and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No representation, undertaking or promise shall be taken to have been given or be implied from anything said or written in negotiations between the parties prior to this Agreement except as expressly stated in this Agreement. Neither party shall have any remedy in respect of any untrue statement made by the other upon which that party relied in entering this Agreement (unless such untrue statement was made fraudulently) and that party's only remedies shall be for breach of contract as provided in this Agreement. The parties agree that any term or condition stated in a Customer purchase order or in any other Customer order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form, (2) this Agreement, and (3) the Documentation. Titles and headings of sections of this Agreement are for convenience only and shall not affect the construction of any provision of this Agreement.

Annex B – HMCTS requirements

5.1.1.1. Compliance Must Haves JFEPS Functional Requirements

User Categories	Description	Approximate Number of Users
System Administrator	Judicial Pay & Expenses Team users with access to all data and all configuration options.	5
Operational	Judicial Pay & Expenses Team users with elevated access to manage reference data and records.	10
Self-Service	Front-end users with access only to their own records and expense/fee claims.	8,492
Clerical	Front-end users witth the facility to process expense/fee claims on behalf of Judicial Office Holders where they have delegated authority to do so.	1,770
Self-Service Approver	Front-end users with access only to their own records and expense/fee claims as well as to the expense/fee claims for other users within their approval line.	250
		10,527

Ref ID	New Area	User Category	Title	Requirement	Goal/Reason	MoSCoW
EF_01	Self-Service, Expenses and Fees	Self-Service	Create an expense or fee claim	To create an expense or fee claim.	So that I can claim an expense or fee.	Must Have
EF_02	Self-Service, Expenses and Fees	Self-Service	Multiple expense and/or fees in a single claim	To enter multiple expense and/or fee claims within a single request. For example entering a fee claim, subsistence claim and mileage claim as separate lines in the same request and submitting them all together, as opposed to having to submit each one separately. Refer to Single Claim & Multi Line Claim document (Single Claim & Multi Line Claim.docx).	So that I can process my claims efficiently by grouping them together rather than creating a single claim for each individual expense or fee.	Must Have
EF_03	Self-Service, Expenses and Fees	Self-Service	Upload required documentation	To upload and attach evidence documents to any line item within an expense or fee claim in any standard format including (but not limited to) png, jpg, pdf, docx, xlsx, msg.	So that approvers can validate the claim by viewing the associated proof.	Must Have

EF_05	Self-Service, Expenses and Fees	Self-Service	Modify an unsubmitted expense or fee claim	To modify an unsubmitted expense or fee claim, including "save and return" capability where a user can save a part completed claim and return to it later to complete it.	So that I can correct or add to my expense or fee claim.	Must Have
EF_06	Self-Service, Expenses and Fees	Self-Service	Delete an unsubmitted expense or fee claim	To delete an unsubmitted expense or fee claim.	So that I can delete an expense or fee claim created by mistake or no longer required, either an entire claim or individual lines within a claim.	Must Have
EF_07	Self-Service, Expenses and Fees	Self-Service	Submit expense or fee claim for approval	To submit an expense or fee claim for approval.	So that my expense or fee claims are approved for payment.	Must Have
EF_08	Self-Service, Expenses and Fees	Self-Service	Self declaration statement	To confirm with each submission that I have declared that the claim meets policy requirements and I accept any liability for false claims. This may be a checkbox or other mechanism for acknowledging a self declaration statement.	So that I acknowledge that I have sole responsibility for making sure my claim is compliant with relevant rules.	Must Have
EF_09	Self-Service, Expenses and Fees	Self-Service	Late claim submission	To confirm I have Regional Office approval for late submission when submitting a claim more than 3 months after the sitting date.	So that approvers know that the late submission had been pre-approved.	Must Have
EF_10	Self-Service, Expenses and Fees	System	Late claim submission evidence	To enforce attachment of evidence document when self-service users confirm approval from Regional Office for late submission of a claim more than 3 months after the sitting date.	So that self-service user must provide documentary evidence to support their assertion that they have approval to proceed with the late claim.	Must Have
EF_11	Self-Service, Expenses and Fees	Self-Service	Un-submit expense or fee claim	To un-submit an expense or fee claim that is pending approval.	So that I can amend the expense or fee claim if necessary.	Must Have
EF_12	Self-Service, Expenses and Fees	Self-Service	View current and historical claims	To view current and historical expense and fee claims, including any attached evidence documents.	So that I can see my expense and fee claim history and any items	Must Have

					awaiting approval or payment.	
EF_13	Self-Service, Expenses and Fees	Self-Service	Amend rejected claims	To amend rejected expense or fee claims, including amendments to individual line items.	So that I can amend a rejected claim rather than having to start it again as a new claim.	Must Have
EF_14	Self-Service, Expenses and Fees	Clerical	Create an expense or fee claim	To create an expense or fee claim on behalf of JOH/NLM. Refer to Information about Clerical Claims document (Information about Clerical Claims.docx).	So that expenses and/or fees are paid to a claimant.	Must Have
EF_15	Self-Service, Expenses and Fees	Clerical	Multiple expense and/or fees in a single claim	To enter multiple expense and/or fee claims within a single request on behalf of JOH/NLM. For example entering a fee claim, subsistence claim and mileage claim as separate lines in the same request and submitting them all together, as opposed to having to submit each one separately.	So that I can process claims efficiently on behalf of others by grouping them together rather than creating a single claim for each individual expense or fee.	Must Have
EF_16	Self-Service, Expenses and Fees	Clerical	Upload required documentation	To upload and attach evidence documents to any line item within an expense or fee claim on behalf of JOH/NLM in any standard format including (but not limited to) png, jpg, pdf, docx, xlsx, msg.	So that approvers can validate the claim by viewing the associated proof.	Must Have
EF_17	Self-Service, Expenses and Fees	Clerical	Modify an unsubmitted expense or fee claim	To modify an unsubmitted fee or expense on behalf of JOH/NLM, including "save and return" capability where a user can save a part completed claim and return to it later to complete it.	So that I can correct or add to an expense or fee claim on behalf of others.	Must Have
EF_18	Self-Service, Expenses and Fees	Clerical	Delete an unsubmitted expense or fee claim	To delete an unsubmitted expense or fee claim on behalf of JOH/NLM.	So that I can delete an expense or fee claim created by mistake or no longer required, either an entire claim or individual lines within a claim.	Must Have
EF_19	Self-Service, Expenses and Fees	Clerical	Submit expense or fee claim for approval	To submit an expense or fee claim for approval on behalf of JOH/NLM.	So that expense or fee claims I raise on behalf of others can be approved for payment.	Must Have

EF_20	Self-Service, Expenses and Fees	Clerical	Self declaration statement	To confirm with each submission that I have declared that the claim meets policy requirements and I accept any liability for false claims. This may be a checkbox or other mechanism for acknowledging a self declaration statement.	So that I acknowledge that I have responsibility for making sure the claim made on behalf of the JOH/NLM is compliant with relevant rules.	Must Have
EF_21	Self-Service, Expenses and Fees	Clerical	Late claim submission	To confirm the JOH/NLM has Regional Office approval for late submission when submitting a claim on behalf of a JOH/NLM more than 3 months after the sitting date.	So that approvers know that the late submission had been pre-approved.	Must Have
EF_22	Self-Service, Expenses and Fees	System	Late claim submission evidence	To enforce attachment of evidence document when clerical users confirm approval from Regional Office for late submission of a claim more than 3 months after the sitting date.	So that clerical user must provide documentary evidence to support the JOH/NLM assertion that they have approval to proceed with the late claim.	Must Have
EF_23	Self-Service, Expenses and Fees	Clerical	Un-submit expense or fee claim	To un-submit an expense or fee claim that is pending approval on behalf of JOH/NLM.	So that I can amend the expense or fee claim made on behalf of others if necessary.	Must Have
EF_24	Self-Service, Expenses and Fees	Clerical	View current and historical claims	To view current and historical expense and fee claims on behalf of JOH/NLM, including any attached evidence documents.	So that I can see expense and fee claim history that I have processed for the JOH/NLM and any items awaiting approval or payment.	Must Have
EF_25	Self-Service, Expenses and Fees	Clerical	Amend rejected claims	To amend rejected expense or fee claims on behalf od JOH/NLM, including amendments to individual line items.	So that I can amend a rejected claim rather than having to start it again as a new claim.	Must Have

EF_28	Self-Service, Expenses and Fees	System	Restrict available values based on JOH appointment	To restrict the values that self-service and clerical users can select when logging fee and expense claims depending on the appointments that are held on their records. Users must only be able to select values that relate to the appointment that the fee or expense relates to.	So that self-service users cannot select values that are not appropriate for the appointment that the claim they are making relates to.	Must Have
EF_29	Self-Service, Expenses and Fees	System	Claim auto check	To automatically prevent a claim that does not meet policy requirements from being submitted.	So that claims that do not meet policy requirements cannot proceed to approval and the self-service user can review and amend the claim.	Must Have
EF_30	Self-Service, Expenses and Fees	System	Identification of duplicate claims	To identify duplicates based on parameters set by the System Administrator. The duplicates may be across multiple-line claims made by different people, or on different dates, or from different sources.	So that duplicate claims are identified accurately.	Must Have
EF_31	Self-Service, Expenses and Fees	System	Flag duplicate claims	To automatically highlight a duplicate expense or fee claim before it is submitted or at the point of submission.	So that the user can correct the claim or update the comments to resolve any misunderstandings.	Must Have
EF_32	Self-Service, Expenses and Fees	System	Prevent submitter from approving claims	To automatically prevent a user who submitted a claim on behalf of a JOH from also approving the same claim.	So that approvers are not approving expense claims that they have submitted themselves.	Must Have
EF_33	Self-Service, Expenses and Fees	System	Email notification - submission	To confirm that the claim has been successfully submitted. For self-service users this would go to the submitter only. For clerical users this would go to the submitter and the JOH/NLM that the claim relates to.	So that I know that the claim submission I have made has been successfully processed.	Must Have
EF_34	Self-Service, Expenses and Fees	Self-Service Approver	View claims awaiting approval	To view submitted expense and fee claims that are awaiting approval.	So that I can check the claim details against the business rules and a sitting record	Must Have

EF_35	Self-Service, Expenses and Fees	Self-Service Approver	Approve claim	To approve submitted expense and fee claims in line with policy.	So that I can approve the claim if it meets policy requirements.	Must Have
EF_36	Self-Service, Expenses and Fees	Self-Service Approver	Reject claim	To reject expense and fee claims that do not align with policy, including the ability to reject specific line items within the claim.	So that I can reject the claim, or part of the claim, if it does not meet policy requirements.	Must Have
EF_37	Self-Service, Expenses and Fees	System	Comments on claim rejection	To enforce approvers (including both Self-Service Approvers and Operational users) rejecting a claim to provide a reason for the rejection. This should include comments/notes as well as a core reason for the rejection selected from a limited list of values.	So that the person who submitted claim can understand why it was rejected.	Must Have
EF_38	Self-Service, Expenses and Fees	System	Automatically adjust approval route	To vary the expense and fee approval process based on whether the JOH is salaried or fee-paid. If the JOH is Fee-Paid the claim must go through approval level one then approval level two. If the JOH is Salaried the claim must bypass approval level one and go directly to approval level two.	So that claims for salaried JOHs are only subject to one level of approval, and claims for fee-paid judges are subject to two levels of approval.	Must Have
EF_39	Self-Service, Expenses and Fees	Operational	Fee and expense limits - additional approval	To have an additional step for the Operational team to approve when a fee or expense limit is exceeded. Refer to Self-Service process diagram (Self Service Process Steps.pdf).	So that I can check that any claims exceeding set limits are valid and can be processed for payment.	Must Have
EF_40	Self-Service, Expenses and Fees	System	Email Notification - rejection	To confirm that the claim has been rejected. For self-service users this would go to the submitter only. For clerical users this would go to the submitter and the JOH/NLM that the claim relates to.	So that I can review the expense or fee claim.	Must Have
EF_41	Self-Service, Expenses and Fees	System	Email Notification - approval	To confirm that the claim has been approved. For self-service users this would go to the submitter only. For clerical users this would go to the submitter and the JOH/NLM that the claim relates to.	So that I know that the claim has been approved and will be paid.	Must Have

EF_42	Self-Service, Expenses and Fees	System	Identify Medical Member sittings	To identify whether an individual sitting record classes as a Medical Member sitting. This could be done using business rules, or be manually identified when the claim is submitted, or come as part of an import from a third party system.	So that Medical Member sittings can be identified and reported.	Must Have
EF_45	Self-Service, Expenses and Fees	System	Record location and associated London Weighting data	To keep a record of the court or tribunal centre at which each sitting took place for each fee claim.	So that the location at which each sitting was completed is held against each individual fee claim.	Must Have
EF_48	Self-Service, Expenses and Fees	System	Assign fee rate	To assign the correct fee rate based on the relevant business rules as defined in the CCalculations Directory (MoJ Judicial Payroll Programme Calculation Directory v1_2.docx) and various policy documents as required.	So that the correct rate is applied to the claim.	Must Have
EF_49	Self-Service, Expenses and Fees	Self-Service	Bank account self-service	Self-service for end users to manage their own bank details.	So that there is a facility for self service maintenance of bank details.	Must Have
EF_53	Self-Service, Expenses and Fees	Self-Service	Bank details prompt	To automatically prompt Self-Service users to enter their bank account details once their user account has been created.	So that self-service users update their bank account details at the earliest opportunity.	Must Have
AC_01	Administration and Configurability	System Administrator	Add new expense and fee types	To add new expense and fee types and associated values, including (but not limited to) name, code, rate, limit and effective date.	So that relevant users have access to the correct expense and fee types to use in their claims.	Must Have
AC_02	Administration and Configurability	System Administrator	Modify existing expense and fee types	To modify existing expense and fee types, including (but not limited to) rate and limit. Rates and limits will change over time so will need to be added to the existing expense or fee type with effective date so that users only see the correct rate for the relevant date.	So that the correct rate and limit details are enforeced on any expense and fee claims.	Must Have

AC_03	Administration and Configurability	System Administrator	Disable expired expense and fee types	To disable existing expense and fee types when they are no longer required, without any impact on current or historical claims.	So that I can remove expense and fee types from circulation without altering historical data or stopping current transactions.	Must Have
AC_04	Administration and Configurability	System Administrator	Configure fee and expense calculations	To configure fee and expense calculation rules.	So that I can implement fee and expense calculation rules based on relevant policies.	Must Have
AC_05	Administration and Configurability	System	Configure fee and expense calculations	To configure fee and expense calculation rules.	So that the supplier can implement fee and expense calculation rules based on relevant policies on behalf of the customer if required.	Must Have
AC_06	Administration and Configurability	System Administrator	Add business rules	To add new business rules based on relevant policies.	So that rules align with current policies and can be applied to new claims.	Must Have
AC_08	Administration and Configurability	System Administrator	Disable expired business rules	To disable existing business rules when they are no longer required, without any impact on current or historical records.	So that I can remove business rules from use without altering historical data or stopping current transactions.	Must Have
AC_10	Administration and Configurability	System Administrator	Configure expense and fee policy rules	To configure the system to automatically flag and prevent a claim from being submitted if it breaches expense or fee policy.	So that claims that do not meet policy requirements cannot proceed to approval and I can investigate the claim and resolve any issues as necessary.	Must Have
AC_11	Administration and Configurability	System Administrator	Add new Cost Centres	To add new cost centres, including (but not limited to) name, code, and effective date.	So that I can add new Cost Centres and associated values in line with business requirements.	Must Have
AC_12	Administration and Configurability	System Administrator	Modify existing Cost Centres	To modify existing cost centres, including (but not limited to) name, code, and effective date.	So that I can amend existing Cost Centres and associated values in line with business requirements.	Must Have

AC_13	Administration and Configurability	System Administrator	Disable expired Cost Centres	To disable existing cost centres when they are no longer required, without any impact on current or historical records.	So that I can remove cost centres from use without altering historical data or stopping current transactions.	Must Have
AC_15	Administration and Configurability	System Administrator	Set duplication rules	To configure data validation and duplicate identification rules.	So that I can control how the system validates data and identifies duplicates.	Must Have
AC_19	Administration and Configurability	System Administrator	Manage available values based on JOH appointment	To manage the configuration of lists of values, including restricting available values based on the values selected in associated parent fields.	So that I can configure the system to be user friendly by only presenting values that are relevant to the information the user is entering	Must Have
AC_20	Administration and Configurability	System	Keep a central list of locations	To have a central list of locations where sittings can take place. This could come from an integration with a central data repository, combined with some manual or bulk data input for additional attributes or additional lines of data.	So that the list of locations and associated attributes can be centrally maintained and used elsewhere in the system.	Must Have
AC_21	Administration and Configurability	System Administrator	Reference data key values	To add key values from feeder systems to reference data tables to allow mapping of correct values.	So that the various key identifier values used in third party feeder systems can be mapped to the correct value in this system.	Must Have
AC_24	Administration and Configurability	System Administrator	Set up notification messages	To create and manage the content and channel for notification messages.	So that I can provide appropriate automated responses to users in line with policy and house style.	Must Have
AC_25	Administration and Configurability	System	Deliver notifications via different channels	To have the capability to deliver notification messages to users by the most appropriate channel, e.g. email, pop-up, push notification etc.	So that users are provided with automated responses via the most appropriate channel for the action.	Must Have

AC_26	Administration and Configurability	Operational / System Administrator	Comprehensive search function	To have a search functionality that allows me to find JOH and fee/expense/payment records by any value held in the record, including (but not limited to) name, NI number, appointment, fee type, expense type, cost centre, salary group, venue.	So that I can easily find the record for the right person based on the information I have available.	Must Have
AC_29	Administration and Configurability	System	Apply updated fee rates	To apply fee rate changes to existing fee claim records from the effective date of the change, regardless of when the new rate is entered. Rate changes are usually entered several months after the effective date of the change and the uplift needs to be applied retrospectively to all fee claims for sittings that have taken place since the effective date. Refer to Information about Fee Rate Changes document (Information about Fee Rate Changes.docx).	So that fee rates are correct and fee records are updated to reflect the new rate.	Must Have
AC_30	Administration and Configurability	Operational	Enter deductions on the system	To enter deduction amounts against relevant pay elements.	So that overpayments can be recovered when necessary.	Must Have
AC_32	Administration and Configurability	System Administrator	Set parameters for data deletion notification routines	To configure the system to produce an automated monthly report of data that is due to be deleted in line with the HMCTS data retention policy.	So that I can receive a regular detailed reminder of data that needs to be removed from the system.	Must Have
BP_01	Batch Processing	System Administrator	Bulk update fee rates	To bulk upload fee rate changes, including the effective date of the change.	So that all relevant fee rates can be updated at the same time rather than having to update each fee rate individually.	Must Have
BP_02	Batch Processing	Operational	Bulk manual import	To manually import expense and fee claims in bulk in various formats, including (but not limited to) csv, xlsx.	So that I can manually import claims in bulk where automated processes are not available.	Must Have

BP_03	Batch Processing	System Administrator	Bulk import failure report	To process bulk data imports and partition off any claim lines that fail validation while importing all lines that pass validation; must automatically produce a report of failed lines. Refer to Bulk Imports & Duplicates document (Process Flow - Bulk Imports & Duplicates.pptx).	So that that the successful lines are imported and ONLY failed lines are reported for fix.	Must Have
BP_04	Batch Processing	System Administrator	Report of failed import lines	To be able to access a report of failed lines from bulk import processes. Refer to Bulk Imports & Duplicates document (Process Flow - Bulk Imports & Duplicates.pptx).	So that I can see the lines that failed to be imported and correct them.	Must Have
BP_05	Batch Processing	Operational	Bulk approval	To bulk approve fee claims that have been entered into the system by self-service or clerical users.	So that claims that have been individually entered do not need to be individually approved but can be processed in bulk to reduce time and effort required.	Must Have
BP_06	Batch Processing	System Administrator	Add new import routines	To add new bulk import routines as required using various source formats, including (but not limited to) txt, JSON, xml, parquet.	So that I can create new bulk import processes in the future if needed.	Must Have
BP_07	Batch Processing	System	Support existing export data formats	To provide export data for current outputs to third party systems in the existing formats (txt, csv, xlsx).	So that existing data output arrangements to third party systems can persist with the new system.	Must Have
BP_08	Batch Processing	System Administrator	Develop new export data in different formats	To configure exports of any and all data held in the system in the formats required by external third parties, including (but not limited to) csv, xlsx, xml, JSON, parquet.	So that data can be exported to other systems successfully.	Must Have
BP_09	Batch Processing	System	Automated API capability within HMCTS	To have the capability to import and export data automatically over API to/from various third party system within HMCTS, including both cloud and on-premise systems. Refer to Integrations List (JFEPS replacement ITT Interfaces v1.xlsx).	So that future development of automated integrations with internal systems can be supported.	Must Have

BP_10	Batch Processing	System	Automated API capability outside HMCTS	To have the capability to import and export data automatically over API to/from various third party system outside HMCTS, including both cloud and on-premise systems. Refer to Integrations List (JFEPS replacement ITT Interfaces v1.xlsx).	So that future development of automated integrations with external systems can be supported.	Must Have
BP_11	Batch Processing	System Administrator	Manual API capability within HMCTS	To have the capability to manually trigger ad-hoc data import and export processes over API to/from various third party system within HMCTS, including both cloud and on-premise systems.	So that future development of manual integrations with internal systems can be supported.	Must Have
BP_12	Batch Processing	System Administrator	Manual API capability outside HMCTS	To have the capability to manually trigger ad-hoc data import and export processes over API to/from various third party system outside HMCTS, including both cloud and on-premise systems.	So that future development of manual integrations with external systems can be supported.	Must Have
PA_02	Person and Appointment	System	Identify primary appointment	To identify a specified Appointment record as the primary appointment. Refer to information about Appointments document (Information about Appointments.docx).	So that I can identify the correct rules to apply to the person based on their primary appointment.	Must Have
PA_04	Person and Appointment	System	Use personal code as the unique identifier	To hold the Personal Code supplied by the HR system as the unique identifier for the person. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that the unique identifier for the person is consistent with the master data from the source system.	Must Have
PA_06	Person and Appointment	System	Hold salary group information	To hold salary group (a short text or numerical identifier to assign the correct group value to the relevant record) for salaried appointments. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that values dependent on salary group can be calculated correctly.	Must Have
PA_07	Person and Appointment	System	Hold FTE salary information	To hold FTE salary amounts for salaried appointments. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that FTE salary figures can be viewed and reported.	Must Have

PA_08	Person and Appointment	System	Hold actual salary information	To hold actual salary amounts for salaried appointments. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that actual salary figures can be viewed and reported.	Must Have
RP_01	Reporting	System Administrator	Monthly Live Reporting	To replicate existing reporting requirements for monthly pay period reports for dissemination to various parts of the organisation and third party providers. Refer to Reporting Requirements document (Reporting Requirements.pdf).	So that operational units and third party partners can continue to receive the reports they need to check individual transactions for each pay period.	Must Have

5.1.1.2. Compliance Must Haves JFEPS NFRs

NFR Ref	Section	Requirement Description	Priority	Link/Reference
NFR_AU_01	Auditability	Audit records must be stored.	Must Have	
NFR_AU_02	Auditability	Audit records must be available for online analysis.	Must Have	
NFR_AU_04	Auditability	Audit trail records must be held against all reference data and data associated with business critical activity and should be able to identify how the data changed.	Must Have	
NFR_AU_05	Auditability	The System must ensure that all user initiated create, update and delete actions are audited.	Must Have	
NFR_AU_06	Auditability	The System must record every end user, system or subsystem or automated actions. a. The date and time of the action b. The user ID of the person who made the change or system ID if the change was system generated c. The information that was actioned d. The data source if the action was system generated e. Any supporting comments if the action was User generated	Must Have	

NFR_AU_07	Auditability	The system must be capable of correlating the audit trail with specific transactions, especially those that impact multiple components. This correlation facilitates efficient analysis and traceability	Must Have	
NFR_AU_09	Auditability	The System must log all errors for the purpose of dealing with support incidents.	Must Have	
NFR_AU_10	Auditability	If applicable, all micro services must be observable, discoverable and calls between microservices traceable.	Must Have	
NFR_AU_11	Auditability	The platform shall be able to present audit data to the customer with the appropriate security permissions to limited users.	Must Have	
NFR_AU_12	Auditability	The Solution to have full stack monitoring in place and real user journey monitoring.	Must Have	
NFR_AV_01	Availability	Repeated running of a transactions must not lead to duplication.	Must Have	
NFR_AV_02	Availability	The system needs to incorporate a high-availability architecture with failover capabilities, leveraging cloud resources (where applicable) for redundancy and resilience, to meet 99.9% availability during Core Operating Hours (08:00 to 20:00) as set out in Call-Off Schedule 14 (Service Levels).	Must Have	
NFR_AV_03	Availability	There shall be no data loss or corruption during normal platform activity. This excludes any event which would constitute a disaster for the purposes of disaster recovery, in which case recovery point and time objectives will apply as set out in section 3 of Call-Off Schedule 8 (Business Continuity and Disaster Recovery).	Must Have	
NFR_AV_04	Availability	Where platform components fail on a fully functional cloud environment, the platform is required to automatically recover the failed node and continue operation without loss of service to its users	Must Have	
NFR_AV_05	Availability	The supplier shall provide availability statistics in line with the availability targets specified within the NFRs and Call-Off Schedules.	Must Have	
NFR_AV_06	Availability	The platform shall have remote monitoring and alerting of all critical components so that the health of the platform can be determined by the supplier without manual intervention or reporting of issues by users.	Must Have	

NFR_AV_07	Availability	All data and statistics available via Supplier dashboards and reports must also be available via API or on-demand. Regular scheduled data exports to be in a common format (e.g.CSV, XML, JSON)	Must Have	
NFR_CS_01	Capacity & Scalability	The system must be scalable in all respects including total number of users, based on the users specified in the Functional Requirements plus 25% growth over the duration of the initial contract, with only configuration changes and no change to core system code and/or product set.	Must Have	Functional Requirements: Users (JFEPS Functional Requirements v1.3.xlsx; "Users" worksheet)
NFR_CS_02	Capacity & Scalability	The system must be scalable in all respects including processing of core business data, as per the JFEPS System Volumetrics documentation (ITT Transaction Time Analysis.pptx) plus 25% growth over the duration of the initial contract, with only configuration changes and no change to core system code and/or product set.	Must Have	JFEPS System Volumetrics (ITT Transaction Time Analysis.pptx)
NFR_CS_03	Capacity & Scalability	The system must be designed so that processes (excluding manual processes) do not take longer regardless of any increases in users, database size and transactions when the system is operating as per the levels detailed in the JFEPS System Volumetrics documentation (ITT Transaction Time Analysis.pptx). Design documents should stipulate expected growth, currently estimated at 25% growth over the duration of the initial contract, and this should be tested for.	Must Have	JFEPS System Volumetrics (ITT Transaction Time Analysis.pptx)
NFR_CS_04	Capacity & Scalability	The platform shall provide the ability to increase the amount of storage available for data as per the JFEPS System Volumetrics documentation levels (Data Migration Outline.xlsx), plus 25% growth over the duration of the initial contract, without fundamental re-engineering of the database or storage tier.	Must Have	JFEPS System Volumetrics (Data Migration Outline.xlsx)
NFR_CL_01	Compliance & Legal	The application must hold data only for as long as is specified by the data retention schedule.	Must Have	JFEPS System Volumetrics (Data Migration Outline.xlsx)
NFR_CL_02	Compliance & Legal	The supplier must ensure that any subcontractors they engage comply fully with current General Data Protection Regulation (GDPR) legislation	Must Have	
NFR_CL_03	Compliance & Legal	The platform shall reside inside the UK boundary	Must Have	

NFR_CL_04	Compliance & Legal	The service provider is to ensure the product meets all necessary accessibility legal requirements as per the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and Equality Act 2010. To meet government accessibility requirements, digital services must: meet level AA of the Web Content Accessibility Guidelines (WCAG 2.2) as a minimum work on the most commonly used assistive technologies - including screen magnifiers, screen readers and speech recognition tools include disabled people in user research have an accessibility statement that explains how accessible the service is - you need to publish this when the service moves into public beta More information can be found at Making your service accessible: an introduction and Understanding accessibility requirements for public sector bodies.	Must Have	Web Content Accessibility Guidelines (WCAG) 2.2
NFR_CL_05	Compliance & Legal	The platform shall comply with GDPR (Part 3 may be relevant), National Cyber Security Centre (NCSC) guidance, and data protection policies (DPA and FoIA) where necessary.	Must Have	
NFR_CL_06	Compliance & Legal	The system and its records shall be compliant with the Gender Recognition Act 2004.	Must Have	
NFR_IN_01	Data & Interoperability	The solution must provide documented secure integration options for future internal and external information systems.	Must Have	
NFR_IN_03	Data & Interoperability	All data accepted by a system interface must be validated before being processed or permanently stored. Transactions containing invalid data must be rejected and the error reported.	Must Have	
NFR_IN_04	Data & Interoperability	All transactions that fail should be either recovered to a consistent state or rolled back in their entirety, so that data entry can be resumed or repeated with the sole use of the end-user applications.	Must Have	
NFR_IN_05	Data & Interoperability	Where a range of valid values for a domain is held by the system or is available for lookup from another system, data must be validated against this after entry and before saving to any persistent data store.	Must Have	

NFR_IN_06	Data & Interoperability	The System must enforce all the maximum and minimum data lengths where defined by the data domain.	Must Have	
NFR_IN_07	Data & Interoperability	Transport failure must not result in loss of data/transaction	Must Have	
NFR_IN_08	Data & Interoperability	The platform must be capable of providing access to all data and functionality through a set of industry standard language and platform independent APIs.	Must Have	
NFR_IN_09	Data & Interoperability	The system shall provide a comprehensive set of language and platform independent events or notifications to enable event-driven integration with other HMCTS systems.	Must Have	
NFR_IN_10	Data & Interoperability	The Solution must provide internal processing controls that assure the integrity of communications between architecture tiers to prevent malicious data in higher tiers exploiting vulnerabilities in lower tiers.	Must Have	
NFR_IN_11	Data & Interoperability	Data that is to be removed from the system must not be recoverable and the method of sanitisation used should be tested to provide assurance of its effectiveness.	Must Have	
NFR_IN_12	Data & Interoperability	The solution will be capable of handling at least all dates between 1900 and 2100, including all date/time changes.	Must Have	
NFR_MA_01	Maintainability	The system must be capable of handling routine business change in a Configurable manner without falling below the applicable Service Levels. Examples of such changes are adding data fields and incremental increases in fee and salary rates.	Must Have	
NFR_MA_02	Maintainability	The System must make provision for reference data updates appropriate to that system, such as Cost Centre Code changes, Post Office Postcode changes or the like, without warranting a code release.	Must Have	
NFR_MA_03	Maintainability	Where relevant, date-based processing must include consideration of Leap Years, Bank Holidays, Short and Long days in all the region(s) covered by the System.	Must Have	
NFR_MA_04	Maintainability	The Solution must provide a secure means of administering cloud infrastructure services.	Must Have	

NFR_MA_05	Maintainability	All changes must have a robust rollback plan and where this is not feasible (due to data integrity, dependancies or other risks), a forward recovery plan that focuses on corrective actions and mitigation (workarounds, fallback plans), must be in place.	Must Have	
NFR_MA_06	Maintainability	It must be possible to configure new monitoring reports, views and alerts as part of continuous service improvement.	Must Have	
NFR_PE_01	Performance	Response times for standard operations (navigation, notifications, submission) must be within 0.25 seconds at maximum load. This includes only elements that the supplier can control within the application itself, and excludes any impact by elements outside of the application, for example network latency.	Must Have	
NFR_PE_03	Performance	The system must be capable of monitoring response times for business transactions and reporting both Network Request Time (NRT) and Software Request Time (SRT).	Must Have	
NFR_PE_04	Performance	The Supplier must demonstrate that the System can provide a response for data retrieval and storage operations of • 90th percentile response time within 1 second • 95th percentile response time within 1.5 seconds • 99th percentile response time within 2 seconds unless specified otherwise within the Business Requirements for the system. This must be tested under realistic load conditions.	Must Have	
NFR_PE_05	Performance	The system must be capable of supporting 2,000 concurrent users.	Must Have	
NFR_PE_06	Performance	System response times should be evaluated at maximum load, excluding network latency. For user operations involving multiple system operations, collaborate with relevant parties to identify latency causes.	Must Have	
NFR_PE_07	Performance	It must be possible to present each metric captured graphically for the purpose of trend analysis from a single interface.	Must Have	
NFR_PE_09	Performance	System must have the capability to monitor the performance of the system in terms of business throughput	Must Have	

NFR_PE_10	Performance	If applicable, infrastructure performance metrics should be available in real-time and historically in one-minute increments over the last 24-hours covering at least the following key components. • CPU utilisation • Memory usage • Disk space • Network latency • Packet loss • Availability • Error rates • Database locks	Must Have	
NFR_PE_11	Performance	Proactive monitoring should be in place to monitor disk use to ensure sufficient disk space is made available for logging, data files, table space etc.	Must Have	
NFR_PE_13	Performance	The supplier shall facilitate performance load testing in test and production environments.	Must Have	
NFR_PE_14	Performance	The solution must monitor resource utilisation at defined intervals and alert to utilisation in excess of defined thresholds and it must be possible to set defined thresholds for utilisation and capacity.	Must Have	
NFR_TE_01	Testability	The supplier shall provide different environments to perform testing at different stages of application development. In addition, in the case of the performance test environment, this shall be a scaled representation of the Live environment.	Must Have	
NFR_TE_02	Testability	The supplier will provide test and production environments.	Must Have	
NFR_US_01	Usability	The System must not return any unhandled errors when responding to an error triggered by a user or system. Error messages must be identified by the System and explained to the user/interfacing system in order to understand the cause of the error.	Must Have	

NFR_US_04	Usability	Services must use generic browser capabiities including but not limited to Mircosoft Edge, Microsoft Internet Explorer, Google Chrome, instead of specific capabilities and/or the use of browser plug-ins that prevents people from using the services	Must Have	
NFR_US_05	Usability	All data captured through a user interface must be validated **on entry** and invalid entries rejected by the user interface, with an explanatory reason to the user.	Must Have	
NFR_US_06	Usability	Where relevent, when a **business logic** error on submission occurs the user should receive an explanatory message indicating what they have done wrong.	Must Have	
NFR_US_07	Usability	Where relevent, when a system error occurs the user should receive an explanatory message indicating that there is something wrong with the system which has not been caused by them; the message will explain what action should be taken the user.	Must Have	
NFR_US_09	Usability	The platform shall have the capability to extend across different operating systems (such as Windows, MacOS) and device types, such PCs, Laptops, tablets and smartphones.	Must Have	
NFR_US_11	Usability	The solution will not require the installation of an executable on the desktop i.e. the solution will be ‘thin client’.	Must Have	

5.1.1.3. JFEPS Functional Requirements

JFEPS Replacement Functional Requirements v1.3; consists of the following contents:
MoSCoW: definition of the Must Have, Should Have, Could Have, Would Have categories used in the Functional Requirements.
Users: definition of the user categories used in the Functional Requirements and Evaluation Questions, and approximate number of users in each category.
Functional Requirements: list of functional requirements for the JFEPS replacement system.

User Categories	**Description**	**Approximate Number of Users**
System Administrator	Judicial Pay & Expenses Team users with access to all data and all configuration options.	5
Operational	Judicial Pay & Expenses Team users with elevated access to manage reference data and records.	10

Self-Service	Front-end users with access only to their own records and expense/fee claims.	8,492
Clerical	Front-end users witth the facility to process expense/fee claims on behalf of Judicial Office Holders where they have delegated authority to do so.	1,770
Self-Service Approver	Front-end users with access only to their own records and expense/fee claims as well as to the expense/fee claims for other users within their approval line.	250
		10,527

Must have	Describes a requirment which must be satisfied in the final solution for the solution to be considered a success	These provide the Minimum Usable Subset (MUS) of requirements which the project guarantees to deliver. This may be defined using some of the following: Cannot deliver on target date without this No point in delivering on target date without this; if it were not delivered, there would be no point deploying the solution on the intended date Not legal without it Unsafe without it Cannot deliver the Business Case without it Ask the question, “what happens if this requirement is not met?” If the answer is “cancel the project – there is no point in implementing a solution that does not meet this requirement” then it is a Must Have requirement. If there is some way round it, even if it is a manual workaround, then it will be a Should Have or a Could Have requirement. Downgrading a requirement to a Should Have or Could Have does not mean it won’t be delivered, simply that delivery is not guaranteed.

Should have	Describes a high priority requirement that should be included in the final solution if it is possible	Important but not vital May be painful to leave out, but the solution is still viable May need some kind of workaround, e.g. management of expectations, some inefficiency, an existing solution, paperwork, etc. A Should Have may be differentiated from a Could Have by reviewing the degree of pain caused by it not being met, in terms of business value or numbers of people affected.
Could have	Describes a requirement which is considered desireable but not necessary	Wanted or desirable but less important Less impact if left out (compared with a Should Have)

Would have	Describes a requirement that stakeholders have agreed will not be implemented as part of the project but would be considered for the future	Placing initiatives in the "would-have" category is one way to help prevent scope creep. If initiatives are in this category, the team knows they are not to be a priority for this specific time frame. Some initiatives in the "won't-have" group will get prioritized in the future, while others are not likely to happen at all. Some teams decide to differentiate between those by creating a subcategory within this group.

Ref ID	New Area	User Category	Title	Requirement	Goal/Reason	MoSCoW
EF_01	Self-Service, Expenses and Fees	Self-Service	Create an expense or fee claim	To create an expense or fee claim.	So that I can claim an expense or fee.	Must Have
EF_02	Self-Service, Expenses and Fees	Self-Service	Multiple expense and/or fees in a single claim	To enter multiple expense and/or fee claims within a single request. For example entering a fee claim, subsistence claim and mileage claim as separate lines in the same request and submitting them all together, as opposed to having to submit each one separately. Refer to Single Claim & Multi Line Claim document (Single Claim & Multi Line Claim.docx).	So that I can process my claims efficiently by grouping them together rather than creating a single claim for each individual expense or fee.	Must Have
EF_03	Self-Service, Expenses and Fees	Self-Service	Upload required documentation	To upload and attach evidence documents to any line item within an expense or fee claim in any standard format including (but not limited to) png, jpg, pdf, docx, xlsx, msg.	So that approvers can validate the claim by viewing the associated proof.	Must Have

EF_04	Self-Service, Expenses and Fees	Self-Service	Comments field on claims	To have the ability to record comments up to 1,000 characters against a claim, including against individual line items, and edit/delete comments in line when editing the claim.	So that I can record additional information to support my claim and clarify any points for the approver.	Should Have
EF_05	Self-Service, Expenses and Fees	Self-Service	Modify an unsubmitted expense or fee claim	To modify an unsubmitted expense or fee claim, including "save and return" capability where a user can save a part completed claim and return to it later to complete it.	So that I can correct or add to my expense or fee claim.	Must Have
EF_06	Self-Service, Expenses and Fees	Self-Service	Delete an unsubmitted expense or fee claim	To delete an unsubmitted expense or fee claim.	So that I can delete an expense or fee claim created by mistake or no longer required, either an entire claim or individual lines within a claim.	Must Have
EF_07	Self-Service, Expenses and Fees	Self-Service	Submit expense or fee claim for approval	To submit an expense or fee claim for approval.	So that my expense or fee claims are approved for payment.	Must Have
EF_08	Self-Service, Expenses and Fees	Self-Service	Self declaration statement	To confirm with each submission that I have declared that the claim meets policy requirements and I accept any liability for false claims. This may be a checkbox or other mechanism for acknowledging a self declaration statement.	So that I acknowledge that I have sole responsibility for making sure my claim is compliant with relevant rules.	Must Have
EF_09	Self-Service, Expenses and Fees	Self-Service	Late claim submission	To confirm I have Regional Office approval for late submission when submitting a claim more than 3 months after the sitting date.	So that approvers know that the late submission had been pre-approved.	Must Have

EF_10	Self-Service, Expenses and Fees	System	Late claim submission evidence	To enforce attachment of evidence document when self-service users confirm approval from Regional Office for late submission of a claim more than 3 months after the sitting date.	So that self-service user must provide documentary evidence to support their assertion that they have approval to proceed with the late claim.	Must Have
EF_11	Self-Service, Expenses and Fees	Self-Service	Un-submit expense or fee claim	To un-submit an expense or fee claim that is pending approval.	So that I can amend the expense or fee claim if necessary.	Must Have
EF_12	Self-Service, Expenses and Fees	Self-Service	View current and historical claims	To view current and historical expense and fee claims, including any attached evidence documents.	So that I can see my expense and fee claim history and any items awaiting approval or payment.	Must Have
EF_13	Self-Service, Expenses and Fees	Self-Service	Amend rejected claims	To amend rejected expense or fee claims, including amendments to individual line items.	So that I can amend a rejected claim rather than having to start it again as a new claim.	Must Have
EF_14	Self-Service, Expenses and Fees	Clerical	Create an expense or fee claim	To create an expense or fee claim on behalf of JOH/NLM. Refer to Information about Clerical Claims document (Information about Clerical Claims.docx).	So that expenses and/or fees are paid to a claimant.	Must Have
EF_15	Self-Service, Expenses and Fees	Clerical	Multiple expense and/or fees in a single claim	To enter multiple expense and/or fee claims within a single request on behalf of JOH/NLM. For example entering a fee claim, subsistence claim and mileage claim as separate lines in the same request and submitting them all together, as opposed to having to submit each one separately.	So that I can process claims efficiently on behalf of others by grouping them together rather than creating a single claim for each individual expense or fee.	Must Have

EF_16	Self-Service, Expenses and Fees	Clerical	Upload required documentation	To upload and attach evidence documents to any line item within an expense or fee claim on behalf of JOH/NLM in any standard format including (but not limited to) png, jpg, pdf, docx, xlsx, msg.	So that approvers can validate the claim by viewing the associated proof.	Must Have
EF_17	Self-Service, Expenses and Fees	Clerical	Modify an unsubmitted expense or fee claim	To modify an unsubmitted fee or expense on behalf of JOH/NLM, including "save and return" capability where a user can save a part completed claim and return to it later to complete it.	So that I can correct or add to an expense or fee claim on behalf of others.	Must Have
EF_18	Self-Service, Expenses and Fees	Clerical	Delete an unsubmitted expense or fee claim	To delete an unsubmitted expense or fee claim on behalf of JOH/NLM.	So that I can delete an expense or fee claim created by mistake or no longer required, either an entire claim or individual lines within a claim.	Must Have
EF_19	Self-Service, Expenses and Fees	Clerical	Submit expense or fee claim for approval	To submit an expense or fee claim for approval on behalf of JOH/NLM.	So that expense or fee claims I raise on behalf of others can be approved for payment.	Must Have
EF_20	Self-Service, Expenses and Fees	Clerical	Self declaration statement	To confirm with each submission that I have declared that the claim meets policy requirements and I accept any liability for false claims. This may be a checkbox or other mechanism for acknowledging a self declaration statement.	So that I acknowledge that I have responsibility for making sure the claim made on behalf of the JOH/NLM is compliant with relevant rules.	Must Have
EF_21	Self-Service, Expenses and Fees	Clerical	Late claim submission	To confirm the JOH/NLM has Regional Office approval for late submission when submitting a claim on behalf of a JOH/NLM more than 3 months after the sitting date.	So that approvers know that the late submission had been pre-approved.	Must Have

EF_22	Self-Service, Expenses and Fees	System	Late claim submission evidence	To enforce attachment of evidence document when clerical users confirm approval from Regional Office for late submission of a claim more than 3 months after the sitting date.	So that clerical user must provide documentary evidence to support the JOH/NLM assertion that they have approval to proceed with the late claim.	Must Have
EF_23	Self-Service, Expenses and Fees	Clerical	Un-submit expense or fee claim	To un-submit an expense or fee claim that is pending approval on behalf of JOH/NLM.	So that I can amend the expense or fee claim made on behalf of others if necessary.	Must Have
EF_24	Self-Service, Expenses and Fees	Clerical	View current and historical claims	To view current and historical expense and fee claims on behalf of JOH/NLM, including any attached evidence documents.	So that I can see expense and fee claim history that I have processed for the JOH/NLM and any items awaiting approval or payment.	Must Have
EF_25	Self-Service, Expenses and Fees	Clerical	Amend rejected claims	To amend rejected expense or fee claims on behalf od JOH/NLM, including amendments to individual line items.	So that I can amend a rejected claim rather than having to start it again as a new claim.	Must Have
EF_26	Self-Service, Expenses and Fees	Self-Service / Clerical	Toggle notifications on / off	To be able to choose whether I receive notifications from the system or not.	So that I can choose whether I receive automated notifications from the system.	Should Have
EF_27	Self-Service, Expenses and Fees	Self-Service / Clerical	Choose notification options	To be able to choose my preferred channel to receive notifications, e.g. email, push notification.	So that I can choose how I receive automated notifications from the system.	Should Have
EF_28	Self-Service, Expenses and Fees	System	Restrict available values based on JOH appointment	To restrict the values that self-service and clerical users can select when logging fee and expense claims depending on the appointments that are held on their records. Users must only be able to select values that relate to the appointment that the fee or expense relates to.	So that self-service users cannot select values that are not appropriate for the appointment that the claim they are making relates to.	Must Have
EF_29	Self-Service, Expenses and Fees	System	Claim auto check	To automatically prevent a claim that does not meet policy	So that claims that do not meet policy requirements cannot proceed to approval	Must Have

				requirements from being submitted.	and the self-service user can review and amend the claim.	
EF_30	Self-Service, Expenses and Fees	System	Identification of duplicate claims	To identify duplicates based on parameters set by the System Administrator. The duplicates may be across multiple-line claims made by different people, or on different dates, or from different sources.	So that duplicate claims are identified accurately.	Must Have
EF_31	Self-Service, Expenses and Fees	System	Flag duplicate claims	To automatically highlight a duplicate expense or fee claim before it is submitted or at the point of submission.	So that the user can correct the claim or update the comments to resolve any misunderstandings.	Must Have
EF_32	Self-Service, Expenses and Fees	System	Prevent submitter from approving claims	To automatically prevent a user who submitted a claim on behalf of a JOH from also approving the same claim.	So that approvers are not approving expense claims that they have submitted themselves.	Must Have
EF_33	Self-Service, Expenses and Fees	System	Email notification - submission	To confirm that the claim has been successfully submitted. For self-service users this would go to the submitter only. For clerical users this would go to the submitter and the JOH/NLM that the claim relates to.	So that I know that the claim submission I have made has been successfully processed.	Must Have
EF_34	Self-Service, Expenses and Fees	Self-Service Approver	View claims awaiting approval	To view submitted expense and fee claims that are awaiting approval.	So that I can check the claim details against the business rules and a sitting record	Must Have
EF_35	Self-Service, Expenses and Fees	Self-Service Approver	Approve claim	To approve submitted expense and fee claims in line with policy.	So that I can approve the claim if it meets policy requirements.	Must Have
EF_36	Self-Service, Expenses and Fees	Self-Service Approver	Reject claim	To reject expense and fee claims that do not align with policy, including the ability to reject specific line items within the claim.	So that I can reject the claim, or part of the claim, if it does not meet policy requirements.	Must Have

EF_37	Self-Service, Expenses and Fees	System	Comments on claim rejection	To enforce approvers (including both Self-Service Approvers and Operational users) rejecting a claim to provide a reason for the rejection. This should include comments/notes as well as a core reason for the rejection selected from a limited list of values.	So that the person who submitted claim can understand why it was rejected.	Must Have
EF_38	Self-Service, Expenses and Fees	System	Automatically adjust approval route	To vary the expense and fee approval process based on whether the JOH is salaried or fee-paid. If the JOH is Fee-Paid the claim must go through approval level one then approval level two. If the JOH is Salaried the claim must bypass approval level one and go directly to approval level two.	So that claims for salaried JOHs are only subject to one level of approval, and claims for fee-paid judges are subject to two levels of approval.	Must Have
EF_39	Self-Service, Expenses and Fees	Operational	Fee and expense limits - additional approval	To have an additional step for the Operational team to approve when a fee or expense limit is exceeded. Refer to Self-Service process diagram (Self Service Process Steps.pdf).	So that I can check that any claims exceeding set limits are valid and can be processed for payment.	Must Have
EF_40	Self-Service, Expenses and Fees	System	Email Notification - rejection	To confirm that the claim has been rejected. For self-service users this would go to the submitter only. For clerical users this would go to the submitter and the JOH/NLM that the claim relates to.	So that I can review the expense or fee claim.	Must Have
EF_41	Self-Service, Expenses and Fees	System	Email Notification - approval	To confirm that the claim has been approved. For self-service users this would go to the submitter only. For clerical users this would go to the submitter and	So that I know that the claim has been approved and will be paid.	Must Have

				the JOH/NLM that the claim relates to.		
EF_42	Self-Service, Expenses and Fees	System	Identify Medical Member sittings	To identify whether an individual sitting record classes as a Medical Member sitting. This could be done using business rules, or be manually identified when the claim is submitted, or come as part of an import from a third party system.	So that Medical Member sittings can be identified and reported.	Must Have
EF_43	Self-Service, Expenses and Fees	System	Running total count of Medical Member sittings	To keep a running total of number of medical member sitting claims per person since 6 April each year.	So that a central record of the number of medical member sittings completed can be automatically maintained.	Should Have
EF_44	Self-Service, Expenses and Fees	System	Calculations based on count of Medical Member sittings	To calculate variable fee rates for individual JOHs based on the number of medical member sittings they have completed since 6 April each year.	So that the rates payable for the sittings can be varied based on the number of sittings completed.	Should Have
EF_45	Self-Service, Expenses and Fees	System	Record location and associated London Weighting data	To keep a record of the court or tribunal centre at which each sitting took place for each fee claim.	So that the location at which each sitting was completed is held against each individual fee claim.	Must Have
EF_46	Self-Service, Expenses and Fees	System	Total count of London Weighting sittings	To keep a total count of the number of sittings each individual undertook at each location within a given financial year.	So that a total number of sittings at London Weighting centres can be calculated.	Should Have

EF_47	Self-Service, Expenses and Fees	System	Calculate London Weighting	To calculate London Weighting retrospectively at the end of each financial year for fee paid JOHs based on the proportion of sittings they have completed at London Weighting centres during the financial year. Refer to information about London Weighting Calculations document (Information about London Weighting Calculations.docx).	So that the retrospective calculation of London Weighting can use the number of sittings completed at London Weighting locations compared with the total number of sittings to establish whether the majority attract London Weighting and the variance for London Weighting should therefore be paid.	Should Have
EF_48	Self-Service, Expenses and Fees	System	Assign fee rate	To assign the correct fee rate based on the relevant business rules as defined in the Calculations Directory (MoJ Judicial Payroll Programme Calculation Directory v1_2.docx) and various policy documents as required.	So that the correct rate is applied to the claim.	Must Have
EF_49	Self-Service, Expenses and Fees	Self-Service	Bank account self-service	Self-service for end users to manage their own bank details.	So that there is a facility for self service maintenance of bank details.	Must Have
EF_50	Self-Service, Expenses and Fees	System	Bank account record	To hold only one set of bank account details for each individual.	So that there is no confusion over which bank account payments should be made to and no issue with retaining old bank account details.	Should Have
EF_51	Self-Service, Expenses and Fees	System	Bank account checking	To automatically check bank account details when they are entered to make sure they are accurate.	So that errors in bank details are minimised.	Should Have
EF_52	Self-Service, Expenses and Fees	System	Bank account change notification	To automatically email confirmation of a change of bank account details to the subject of the change.	So that users have confirmation of a change they have made or notification that a change has been made on their behalf.	Should Have

EF_53	Self-Service, Expenses and Fees	Self-Service	Bank details prompt	To automatically prompt Self-Service users to enter their bank account details once their user account has been created.	So that self-service users update their bank account details at the earliest opportunity.	Must Have
EF_54	Self-Service, Expenses and Fees	System	Prevent users from submitting claims when no bank details present	To prevent self-service users from submitting any claims if bank details have not been provided to pay the claims into.	So that users cannot attempt to raise a claim before a destination bank account is made available.	Should Have
AC_01	Administration and Configurability	System Administrator	Add new expense and fee types	To add new expense and fee types and associated values, including (but not limited to) name, code, rate, limit and effective date.	So that relevant users have access to the correct expense and fee types to use in their claims.	Must Have
AC_02	Administration and Configurability	System Administrator	Modify existing expense and fee types	To modify existing expense and fee types, including (but not limited to) rate and limit. Rates and limits will change over time so will need to be added to the existing expense or fee type with effective date so that users only see the correct rate for the relevant date.	So that the correct rate and limit details are enforeced on any expense and fee claims.	Must Have
AC_03	Administration and Configurability	System Administrator	Disable expired expense and fee types	To disable existing expense and fee types when they are no longer required, without any impact on current or historical claims.	So that I can remove expense and fee types from circulation without altering historical data or stopping current transactions.	Must Have
AC_04	Administration and Configurability	System Administrator	Configure fee and expense calculations	To configure fee and expense calculation rules.	So that I can implement fee and expense calculation rules based on relevant policies.	Must Have

AC_05	Administration and Configurability	System	Configure fee and expense calculations	To configure fee and expense calculation rules.	So that the supplier can implement fee and expense calculation rules based on relevant policies on behalf of the customer if required.	Must Have
AC_06	Administration and Configurability	System Administrator	Add business rules	To add new business rules based on relevant policies.	So that rules align with current policies and can be applied to new claims.	Must Have
AC_07	Administration and Configurability	System Administrator	Edit business rules	To edit existing business rules based on relevant policies, without any impact on current or historical records.	So that rules align with current policies and can be applied to new claims without altering historical data or stopping current transactions.	Should Have
AC_08	Administration and Configurability	System Administrator	Disable expired business rules	To disable existing business rules when they are no longer required, without any impact on current or historical records.	So that I can remove business rules from use without altering historical data or stopping current transactions.	Must Have
AC_09	Administration and Configurability	System Administrator	Delete business rules	To delete existing business rules that are no longer applicable, without any impact on current or historical records.	So that any obsolete rules are not enforced by the system.	Should Have
AC_10	Administration and Configurability	System Administrator	Configure expense and fee policy rules	To configure the system to automatically flag and prevent a claim from being submitted if it breaches expense or fee policy.	So that claims that do not meet policy requirements cannot proceed to approval and I can investigate the claim and resolve any issues as necessary.	Must Have
AC_11	Administration and Configurability	System Administrator	Add new Cost Centres	To add new cost centres, including (but not limited to) name, code, and effective date.	So that I can add new Cost Centres and associated values in line with business requirements.	Must Have
AC_12	Administration and Configurability	System Administrator	Modify existing Cost Centres	To modify existing cost centres, including (but not limited to) name, code, and effective date.	So that I can amend existing Cost Centres and associated values in line with business requirements.	Must Have
AC_13	Administration and Configurability	System Administrator	Disable expired Cost Centres	To disable existing cost centres when they are no longer required, without any impact on current or historical records.	So that I can remove cost centres from use without altering historical data or stopping current transactions.	Must Have

AC_14	Administration and Configurability	System	Restrict available Cost Centre values	To restrict the cost centre values that users can select depending on other details associated with the record. Users must only be able to select cost centre values that relate to the appointment, location, tribunal etc. that the fee or expense relates to.	So that users cannot select cost centre values that are not appropriate for the claim they relate to.	Should Have
AC_15	Administration and Configurability	System Administrator	Set duplication rules	To configure data validation and duplicate identification rules.	So that I can control how the system validates data and identifies duplicates.	Must Have
AC_16	Administration and Configurability	System Administrator	Bulk update pay element codes	To bulk upload new pay element codes.	So that new pay element codes can be added in bulk rather than individually to save time and effort.	Should Have
AC_17	Administration and Configurability	System Administrator	Bulk allocate pay element codes	To bulk allocate pay element codes to individual JOH records if necessary.	So that pay element codes can be assigned to individual records if required in bulk rather than individually updated each record.	Should Have
AC_18	Administration and Configurability	System Administrator	Disable expired pay element codes	To bulk disable decommissioned pay element codes, without impacting on active expense and fee claims utilising the outgoing codes.	So that expired pay element codes can be taken out of circulation without impacting on existing records.	Should Have
AC_19	Administration and Configurability	System Administrator	Manage available values based on JOH appointment	To manage the configuration of lists of values, including restricting available values based on the values selected in associated parent fields.	So that I can configure the system to be user friendly by only presenting values that are relevant to the information the user is entering	Must Have
AC_20	Administration and Configurability	System	Keep a central list of locations	To have a central list of locations where sittings can take place. This could come from an integration with a central data repository, combined with some manual or bulk data input for additional attributes or additional lines of data.	So that the list of locations and associated attributes can be centrally maintained and used elsewhere in the system.	Must Have

AC_21	Administration and Configurability	System Administrator	Reference data key values	To add key values from feeder systems to reference data tables to allow mapping of correct values.	So that the various key identifier values used in third party feeder systems can be mapped to the correct value in this system.	Must Have
AC_22	Administration and Configurability	Operational	Create expense claim automatically	To automatically generate expense and fee claims from scanned hard-copy fee and expense claim forms.	So that I do not have to manually enter information from hard-copy claim forms.	Should Have
AC_23	Administration and Configurability	Operational	Attach documents to a claim record	To upload and attach evidence documents to any line item within an expense or fee claim in any standard format including (but not limited to) png, jpg, pdf, docx, xlsx, msg.	So that the associated proof for the claim is held with the claim record.	Should Have
AC_24	Administration and Configurability	System Administrator	Set up notification messages	To create and manage the content and channel for notification messages.	So that I can provide appropriate automated responses to users in line with policy and house style.	Must Have
AC_25	Administration and Configurability	System	Deliver notifications via different channels	To have the capability to deliver notification messages to users by the most appropriate channel, e.g. email, pop-up, push notification etc.	So that users are provided with automated responses via the most appropriate channel for the action.	Must Have
AC_26	Administration and Configurability	Operational / System Administrator	Comprehensive search function	To have a search functionality that allows me to find JOH and fee/expense/payment records by any value held in the record, including (but not limited to) name, NI number, appointment, fee type, expense type, cost centre, salary group, venue.	So that I can easily find the record for the right person based on the information I have available.	Must Have

AC_27	Administration and Configurability	Operational / System Administrator	Comprehensive view function	To have functionality that allows me to view grouped JOH and fee/expense/payment records based on any value or cobmination of values held in the record, including (but not limited to) name, NI number, appointment, fee type, expense type, cost centre, salary group, venue. Views should be interractive so that individual and bulk actions (e.g. update to a specific field on each selected record) can be carried out from the view.	So that I can view grouped data and carry out individual and bulk actions directly from the view.	Should Have
AC_28	Administration and Configurability	Operational / System Administrator	Comprehensive filter function	To have functionality that allows me to filter JOH and fee/expense/payment records in views and reports based on any value or combination of values held in the record, including (but not limited to) date range, name, NI number, appointment, fee type, expense type, cost centre, salary group, venue.	So that I can filter views and reports to find the record or group of records that I need to work with.	Should Have
AC_29	Administration and Configurability	System	Apply updated fee rates	To apply fee rate changes to existing fee claim records from the effective date of the change, regardless of when the new rate is entered. Rate changes are usually entered several months after the effective date of the change and the uplift needs to be applied retrospectively to all fee claims for sittings that have taken place since the effective date. Refer to Information about Fee Rate Changes document	So that fee rates are correct and fee records are updated to reflect the new rate.	Must Have

				(Information about Fee Rate Changes.docx).		
AC_30	Administration and Configurability	Operational	Enter deductions on the system	To enter deduction amounts against relevant pay elements.	So that overpayments can be recovered when necessary.	Must Have
AC_31	Administration and Configurability	System	Support overpayment management	To support the overpayment recovery process. Refer to Overpayment Recovery Process diagram (Overpayment Recovery Process.pdf).	So that the manual monitoring and data entry required for overpayment recovery can be reduced.	Could Have
AC_32	Administration and Configurability	System Administrator	Set parameters for data deletion notification routines	To configure the system to produce an automated monthly report of data that is due to be deleted in line with the HMCTS data retention policy.	So that I can receive a regular detailed reminder of data that needs to be removed from the system.	Must Have
AC_33	Administration and Configurability	System Administrator	Manual bulk deletion facility	To be able to select data items and records that need to be deleted, review the selection, and delete them in bulk.	So that I can review data before it is deleted and have full control of what is removed from the system.	Should Have
AC_34	Administration and Configurability	System	Bulk deletion confirmation	To have a final confirmation stage before a bulk deletion event is processed.	So that bulk deletion of data is not completed in error, e.g. if the wrong button is clicked accidentally.	Should Have
AC_35	Administration and Configurability	System	Archiving for system performance	To automatically move data that is not required for day-to-day live reporting and calculations to an internal archive, where it is still retrievable and reportable.	So that system performance is optimised by not processing data that is not required for the process, but data is retained in an accessible manner.	Should Have

AC_36	Administration and Configurability	System Administrator	Set parameters export to HMCTS archive	To configure the system to automatically export historical data to the HMCTS archive system (ARM) in line with HMCTS data retention policy.	So that historical data can be retained and accessed appriately.	Should Have
BP_01	Batch Processing	System Administrator	Bulk update fee rates	To bulk upload fee rate changes, including the effective date of the change.	So that all relevant fee rates can be updated at the same time rather than having to update each fee rate individually.	Must Have
BP_02	Batch Processing	Operational	Bulk manual import	To manually import expense and fee claims in bulk in various formats, including (but not limited to) csv, xlsx.	So that I can manually import claims in bulk where automated processes are not available.	Must Have
BP_03	Batch Processing	System Administrator	Bulk import failure report	To process bulk data imports and partition off any claim lines that fail validation while importing all lines that pass validation; must automatically produce a report of failed lines. Refer to Bulk Imports & Duplicates document (Process Flow - Bulk Imports & Duplicates.pptx).	So that that the successful lines are imported and ONLY failed lines are reported for fix.	Must Have
BP_04	Batch Processing	System Administrator	Report of failed import lines	To be able to access a report of failed lines from bulk import processes. Refer to Bulk Imports & Duplicates document (Process Flow - Bulk Imports & Duplicates.pptx).	So that I can see the lines that failed to be imported and correct them.	Must Have
BP_05	Batch Processing	Operational	Bulk approval	To bulk approve fee claims that have been entered into the system by self-service or clerical users.	So that claims that have been individually entered do not need to be individually approved but can be processed in bulk to reduce time and effort required.	Must Have
BP_06	Batch Processing	System Administrator	Add new import routines	To add new bulk import routines as required using various source formats, including (but not limited to) txt, JSON, xml, parquet.	So that I can create new bulk import processes in the future if needed.	Must Have

BP_07	Batch Processing	System	Support existing export data formats	To provide export data for current outputs to third party systems in the existing formats (txt, csv, xlsx).	So that existing data output arrangements to third party systems can persist with the new system.	Must Have
BP_08	Batch Processing	System Administrator	Develop new export data in different formats	To configure exports of any and all data held in the system in the formats required by external third parties, including (but not limited to) csv, xlsx, xml, JSON, parquet.	So that data can be exported to other systems successfully.	Must Have
BP_09	Batch Processing	System	Automated API capability within HMCTS	To have the capability to import and export data automatically over API to/from various third party system within HMCTS, including both cloud and on-premise systems. Refer to Integrations List (JFEPS replacement ITT Interfaces v1.xlsx).	So that future development of automated integrations with internal systems can be supported.	Must Have
BP_10	Batch Processing	System	Automated API capability outside HMCTS	To have the capability to import and export data automatically over API to/from various third party system outside HMCTS, including both cloud and on-premise systems. Refer to Integrations List (JFEPS replacement ITT Interfaces v1.xlsx).	So that future development of automated integrations with external systems can be supported.	Must Have
BP_11	Batch Processing	System Administrator	Manual API capability within HMCTS	To have the capability to manually trigger ad-hoc data import and export processes over API to/from various third party system within HMCTS, including both cloud and on-premise systems.	So that future development of manual integrations with internal systems can be supported.	Must Have

BP_12	Batch Processing	System Administrator	Manual API capability outside HMCTS	To have the capability to manually trigger ad-hoc data import and export processes over API to/from various third party system outside HMCTS, including both cloud and on-premise systems.	So that future development of manual integrations with external systems can be supported.	Must Have
PA_01	Person and Appointment	System	JOH records structure	To hold JOH records in the same way as they are held in Judicial HR, which is one single record for the person, with one or more associated appointment records. Refer to information about Appointments document (Information about Appointments.docx).	So that data structures are consistent across the data landscape to simplify integration.	Should Have
PA_02	Person and Appointment	System	Identify primary appointment	To identify a specified Appointment record as the primary appointment. Refer to information about Appointments document (Information about Appointments.docx).	So that I can identify the correct rules to apply to the person based on their primary appointment.	Must Have
PA_03	Person and Appointment	System	Copy key primary appointment data to the person record	To automatically copy given data fields from the primary Appointment record to the Person record when the primary Appointment record is created, updated or closed.	So that key information about the primary appointment is immediately available to me without having to drill-down into the record.	Should Have
PA_04	Person and Appointment	System	Use personal code as the unique identifier	To hold the Personal Code supplied by the HR system as the unique identifier for the person. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that the unique identifier for the person is consistent with the master data from the source system.	Must Have

PA_05	Person and Appointment	System	Hold multiple identifiers	To hold multiple identifiers on each appointment record. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that items from third party systems that us different unique identifiers can be mapped correctly.	Should Have
PA_06	Person and Appointment	System	Hold salary group information	To hold salary group (a short text or numerical identifier to assign the correct group value to the relevant record) for salaried appointments. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that values dependent on salary group can be calculated correctly.	Must Have
PA_07	Person and Appointment	System	Hold FTE salary information	To hold FTE salary amounts for salaried appointments. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that FTE salary figures can be viewed and reported.	Must Have
PA_08	Person and Appointment	System	Hold actual salary information	To hold actual salary amounts for salaried appointments. Refer to Conceptual Data Model (ITT Conceptual Data Models.pdf).	So that actual salary figures can be viewed and reported.	Must Have
RP_01	Reporting	System Administrator	Monthly Live Reporting	To replicate existing reporting requirements for monthly pay period reports for dissemination to various parts of the organisation and third party providers. Refer to Reporting Requirements document (Reporting Requirements.pdf).	So that operational units and third party partners can continue to receive the reports they need to check individual transactions for each pay period.	Must Have
RP_02	Reporting	Operational / System Administrator	Bespoke reports	To have the ability to create bespoke reports & dashboards to my requirements using any and all data available to me in the system.	So that I can report on all the data that I need to report on in the way that it most appropriate to my needs.	Should Have

RP_03	Reporting	System	Operational Reporting	To support development of integration to the Strategic Data Platform (SDP) over API for aggregated reporting. Refer to Reporting Requirements document (Reporting Requirements.pdf).	So that HMCTS can develop their operational reporting capability.	Should Have
RP_04	Reporting	Operational	Validation reports	To have reports to hightlight any anamolies in the data or highlight any duplicates or missing data.	So that I can see where issues are and contact the user to correct them.	Should Have

5.1.1.4. JFEPS Non-Functional Requirements

Provides a list of Non-Functional Requirements for the JFEPS replacement system.

Must Have	Describes a requirment which Must Have be satisfied in the final solution for the solution to be considered a success	These provide the Minimum Usable Subset (MUS) of requirements which the project guarantees to deliver. This may be defined using some of the following: Cannot deliver on target date without this No point in delivering on target date without this; if it were not delivered, there would be no point deploying the solution on the intended date Not legal without it Unsafe without it Cannot deliver the Business Case without it Ask the question, “what happens if this requirement is not met?” If the answer is “cancel the project – there is no point in implementing a solution that does not meet this requirement” then it is a Must Have requirement. If there is some way round it, even if it is a manual workaround, then it will be a Should Have or a Could Have requirement. Downgrading a requirement to a Should Have or Could Have does not mean it won’t be delivered, simply that delivery is not guaranteed.

Should Have	Describes a high priority requirement that Should Have be included in the final solution if it is possible	Important but not vital May be painful to leave out, but the solution is still viable May need some kind of workaround, e.g. management of expectations, some inefficiency, an existing solution, paperwork, etc. A Should Have may be differentiated from a Could Have by reviewing the degree of pain caused by it not being met, in terms of business value or numbers of people affected.

Could have	Describes a requirement which is considered desireable but not necessary	Wanted or desirable but less important Less impact if left out (compared with a Should Have)

Would have	Describes a requirement that stakeholders have agreed will not be implemented as part of the project but would be considered for the future	Placing initiatives in the “would-have” category is one way to help prevent scope creep. If initiatives are in this category, the team knows they are not to be a priority for this specific time frame. Some initiatives in the “won't-have” group will get prioritized in the future, while others are not likely to happen at all. Some teams decide to differentiate between those by creating a subcategory within this group.

NFR Ref	Section	Requirement Description	Priority	Link/Reference
NFR_AU_01	Auditability	Audit records must be stored.	Must Have	
NFR_AU_02	Auditability	Audit records must be available for online analysis.	Must Have	
NFR_AU_03	Auditability	HMCTS should be able to determine the frequency of storage/deletion of all audit records.	Should Have	
NFR_AU_04	Auditability	Audit trail records must be held against all reference data and data associated with business critical activity and should be able to identify how the data changed.	Must Have	
NFR_AU_05	Auditability	The System must ensure that all user initiated create, update and delete actions are audited.	Must Have	

NFR_AU_06	Auditability	The System must record every end user, system or subsystem or automated actions. a. The date and time of the action b. The user ID of the person who made the change or system ID if the change was system generated c. The information that was actioned d. The data source if the action was system generated e. Any supporting comments if the action was User generated	Must Have	
NFR_AU_07	Auditability	The system must be capable of correlating the audit trail with specific transactions, especially those that impact multiple components. This correlation facilitates efficient analysis and traceability	Must Have	
NFR_AU_08	Auditability	The Service Provider must ensure that the applications error logs are accessible and in a format that is searchable and reportable for analysis.	Should Have	
NFR_AU_09	Auditability	The System must log all errors for the purpose of dealing with support incidents.	Must Have	
NFR_AU_10	Auditability	If applicable, all micro services must be observable, discoverable and calls between microservices traceable.	Must Have	
NFR_AU_11	Auditability	The platform shall be able to present audit data to the customer with the appropriate security permissions to limited users.	Must Have	
NFR_AU_12	Auditability	The Solution to have full stack monitoring in place and real user journey monitoring.	Must Have	
NFR_AV_01	Availability	Repeated running of a transactions must not lead to duplication.	Must Have	
NFR_AV_02	Availability	The system needs to incorporate a high-availability architecture with failover capabilities, leveraging cloud resources (where applicable) for redundancy and resilience, to meet 99.9% availability during Core Operating Hours (08:00 to 20:00) as set out in Call-Off Schedule 14 (Service Levels).	Must Have	

NFR_AV_03	Availability	There shall be no data loss or corruption during normal platform activity. This excludes any event which would constitute a disaster for the purposes of disaster recovery, in which case recovery point and time objectives will apply as set out in section 3 of Call-Off Schedule 8 (Business Continuity and Disaster Recovery).	Must Have	
NFR_AV_04	Availability	Where platform components fail on a fully functional cloud environment, the platform is required to automatically recover the failed node and continue operation without loss of service to its users	Must Have	
NFR_AV_05	Availability	The supplier shall provide availability statistics in line with the availability targets specified within the NFRs and Call-Off Schedules.	Must Have	
NFR_AV_06	Availability	The platform shall have remote monitoring and alerting of all critical components so that the health of the platform can be determined by the supplier without manual intervention or reporting of issues by users.	Must Have	
NFR_AV_07	Availability	All data and statistics available via Supplier dashboards and reports must also be available via API or on-demand. Regular scheduled data exports to be in a common format (e.g.CSV, XML, JSON)	Must Have	
NFR_CS_01	Capacity & Scalability	The system must be scalable in all respects including total number of users, based on the users specified in the Functional Requirements plus 25% growth over the duration of the initial contract, with only configuration changes and no change to core system code and/or product set.	Must Have	Functional Requirements: Users (JFEPS Functional Requirements v1.3.xlsx; "Users" worksheet)
NFR_CS_02	Capacity & Scalability	The system must be scalable in all respects including processing of core business data, as per the JFEPS System Volumetrics documentation (ITT Transaction Time Analysis.pptx) plus 25% growth over the duration of the initial contract, with only configuration changes and no change to core system code and/or product set.	Must Have	JFEPS System Volumetrics (ITT Transaction Time Analysis.pptx)

NFR_CS_03	Capacity & Scalability	The system must be designed so that processes (excluding manual processes) do not take longer regardless of any increases in users, database size and transactions when the system is operating as per the levels detailed in the JFEPS System Volumetrics documentation (ITT Transaction Time Analysis.pptx). Design documents should stipulate expected growth, currently estimated at 25% growth over the duration of the initial contract, and this should be tested for.	Must Have	JFEPS System Volumetrics (ITT Transaction Time Analysis.pptx)
NFR_CS_04	Capacity & Scalability	The platform shall provide the ability to increase the amount of storage available for data as per the JFEPS System Volumetrics documentation levels (Data Migration Outline.xlsx), plus 25% growth over the duration of the initial contract, without fundamental re-engineering of the database or storage tier.	Must Have	JFEPS System Volumetrics (Data Migration Outline.xlsx)
NFR_CL_01	Compliance & Legal	The application must hold data only for as long as is specified by the data retention schedule.	Must Have	JFEPS System Volumetrics (Data Migration Outline.xlsx)
NFR_CL_02	Compliance & Legal	The supplier must ensure that any subcontractors they engage comply fully with current General Data Protection Regulation (GDPR) legislation	Must Have	
NFR_CL_03	Compliance & Legal	The platform shall reside inside the UK boundary	Must Have	
NFR_CL_04	Compliance & Legal	The service provider is to ensure the product meets all necessary accessibility legal requirements as per the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and Equality Act 2010. To meet government accessibility requirements, digital services must: meet level AA of the Web Content Accessibility Guidelines (WCAG 2.2) as a minimum work on the most commonly used assistive technologies - including screen magnifiers, screen readers and speech recognition tools include disabled people in user research have an accessibility statement that explains how accessible the service is - you need to publish this when the service moves into public beta More information can be found at Making your service accessible: an introduction and Understanding accessibility requirements for public sector bodies.	Must Have	Web Content Accessibility Guidelines (WCAG) 2.2
NFR_CL_05	Compliance & Legal	The platform shall comply with GDPR (Part 3 may be relevant), National Cyber Security Centre (NCSC) guidance, and data protection policies (DPA and FoIA) where necessary.	Must Have	

NFR_CL_06	Compliance & Legal	The system and its records shall be compliant with the Gender Recognition Act 2004.	Must Have	
NFR_IN_01	Data & Interoperability	The solution must provide documented secure integration options for future internal and external information systems.	Must Have	
NFR_IN_02	Data & Interoperability	The migration architecture should support parallel processing and distributed systems if required for efficient data transfer	Should Have	
NFR_IN_03	Data & Interoperability	All data accepted by a system interface must be validated before being processed or permanently stored. Transactions containing invalid data must be rejected and the error reported.	Must Have	
NFR_IN_04	Data & Interoperability	All transactions that fail should be either recovered to a consistent state or rolled back in their entirety, so that data entry can be resumed or repeated with the sole use of the end-user applications.	Must Have	
NFR_IN_05	Data & Interoperability	Where a range of valid values for a domain is held by the system or is available for lookup from another system, data must be validated against this after entry and before saving to any persistent data store.	Must Have	
NFR_IN_06	Data & Interoperability	The System must enforce all the maximum and minimum data lengths where defined by the data domain.	Must Have	
NFR_IN_07	Data & Interoperability	Transport failure must not result in loss of data/transaction	Must Have	
NFR_IN_08	Data & Interoperability	The platform must be capable of providing access to all data and functionality through a set of industry standard language and platform independent APIs.	Must Have	
NFR_IN_09	Data & Interoperability	The system shall provide a comprehensive set of language and platform independent events or notifications to enable event-driven integration with other HMCTS systems.	Must Have	
NFR_IN_10	Data & Interoperability	The Solution must provide internal processing controls that assure the integrity of communications between architecture tiers to prevent malicious data in higher tiers exploiting vulnerabilities in lower tiers.	Must Have	
NFR_IN_11	Data & Interoperability	Data that is to be removed from the system must not be recoverable and the method of sanitisation used should be tested to provide assurance of its effectiveness.	Must Have	

NFR_IN_12	Data & Interoperability	The solution will be capable of handling at least all dates between 1900 and 2100, including all date/time changes.	Must Have	
NFR_IN_13	Data & Interoperability	It will be possible to “copy and paste” data within the solution to avoid rekeying information, as well as ability to copy from a system field and pasting into another application.	Should Have	
NFR_DM_01	Data Migration	The system should be capable of ingesting data for the purposes of data migration from multiple sources to a new system.	Should Have	
NFR_DM_02	Data Migration	Data validation mechanisms should be in place to detect and handle any inconsistencies or errors in the migrated data	Should Have	
NFR_DM_03	Data Migration	The system should be capable of handling large volumes of data migration, in line with JFEPS System Volumetrics documentation levels (Data Migration Outline.xlsx), without performance degradation greater than 20% variance to normal performance measurements.	Should Have	
NFR_DM_04	Data Migration	The migration process should incorporate mechanisms to handle and log any errors or exceptions encountered during the data transfer	Should Have	
NFR_DM_05	Data Migration	Detailed error messages should be generated to assist in troubleshooting and resolving migration issues	Should Have	
NFR_DM_06	Data Migration	Regular backups of both the source and target data should be taken through out the duration of the data migration to ensure data recoverability in case of migration failures	Should Have	
NFR_DM_07	Data Migration	Regulatory requirements or industry-specific guidelines for data migration should be adhered to, if applicable	Should Have	
NFR_DR_01	Disaster Recovery & Business Continuity	The platform must be geo-resilient. It must be able to run the services from more than one UK region	Could Have	
NFR_DR_02	Disaster Recovery & Business Continuity	The platform at any secondary data centre site should be regression tested quarterly or following the production release onto the site whichever comes first if not in live use as a result of architectural design and whenever there are changes that can impact the disaster recovery.	Should Have	

NFR_MA_01	Maintainability	The system must be capable of handling routine business change in a Configurable manner without falling below the applicable Service Levels. Examples of such changes are adding data fields and incremental increases in fee and salary rates.	Must Have	
NFR_MA_02	Maintainability	The System must make provision for reference data updates appropriate to that system, such as Cost Centre Code changes, Post Office Postcode changes or the like, without warranting a code release.	Must Have	
NFR_MA_03	Maintainability	Where relevant, date-based processing must include consideration of Leap Years, Bank Holidays, Short and Long days in all the region(s) covered by the System.	Must Have	
NFR_MA_04	Maintainability	The Solution must provide a secure means of administering cloud infrastructure services.	Must Have	
NFR_MA_05	Maintainability	All changes must have a robust rollback plan and where this is not feasible (due to data integrity, dependancies or other risks), a forward recovery plan that focuses on corrective actions and mitigation (workarounds, fallback plans), must be in place.	Must Have	
NFR_MA_06	Maintainability	It must be possible to configure new monitoring reports, views and alerts as part of continuous service improvement.	Must Have	
NFR_PE_01	Performance	Response times for standard operations (navigation, notifications, submission) must be within 0.25 seconds at maximum load. This includes only elements that the supplier can control within the application itself, and excludes any impact by elements outside of the application, for example network latency.	Must Have	
NFR_PE_02	Performance	Self-Service user and 3rd party facing services must be tested with a bandwidth download restriction of 10Mbps and upload restriction of 1Mbps.	Should Have	
NFR_PE_03	Performance	The system must be capable of monitoring response times for business transactions and reporting both Network Request Time (NRT) and Software Request Time (SRT).	Must Have	

NFR_PE_04	Performance	The Supplier must demonstrate that the System can provide a response for data retrieval and storage operations of • 90th percentile response time within 1 second • 95th percentile response time within 1.5 seconds • 99th percentile response time within 2 seconds unless specified otherwise within the Business Requirements for the system. This must be tested under realistic load conditions.	Must Have	
NFR_PE_05	Performance	The system must be capable of supporting 2,000 concurrent users.	Must Have	
NFR_PE_06	Performance	System response times should be evaluated at maximum load, excluding network latency. For user operations involving multiple system operations, collaborate with relevant parties to identify latency causes.	Must Have	
NFR_PE_07	Performance	It must be possible to present each metric captured graphically for the purpose of trend analysis from a single interface.	Must Have	
NFR_PE_08	Performance	The System should log and store performance metrics.	Should Have	
NFR_PE_09	Performance	System must have the capability to monitor the performance of the system in terms of business throughput	Must Have	
NFR_PE_10	Performance	If applicable, infrastructure performance metrics should be available in real-time and historically in one-minute increments over the last 24-hours covering at least the following key components. • CPU utilisation • Memory usage • Disk space • Network latency • Packet loss • Availability • Error rates • Database locks	Must Have	
NFR_PE_11	Performance	Proactive monitoring should be in place to monitor disk use to ensure sufficient disk space is made available for logging, data files, table space etc.	Must Have	

NFR_PE_12	Performance	The platform will provide the capability of delivering status messages to client's browsers at a speed of near real time at peak load.	Should Have	
NFR_PE_13	Performance	The supplier shall facilitate performance load testing in test and production environments.	Must Have	
NFR_PE_14	Performance	The solution must monitor resource utilisation at defined intervals and alert to utilisation in excess of defined thresholds and it must be possible to set defined thresholds for utilisation and capacity.	Must Have	
NFR_TE_01	Testability	The supplier shall provide different environments to perform testing at different stages of application development. In addition, in the case of the performance test environment, this shall be a scaled representation of the Live environment.	Must Have	
NFR_TE_02	Testability	The supplier will provide test and production environments.	Must Have	
NFR_US_01	Usability	The System must not return any unhandled errors when responding to an error triggered by a user or system. Error messages must be identified by the System and explained to the user/interfacing system in order to understand the cause of the error.	Must Have	
NFR_US_02	Usability	Services must be universally accessible and must support the Accessibility Tooling as identified by GDS. https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps	Should Have	Understanding accessibility requirements for public sector bodies
NFR_US_03	Usability	The system must be accessible to office based and remote JOH and HMCTS users. https://www.gov.uk/service-manual/technology/using-progressive-enhancement#testing-your-service	Should Have	Building a resilient frontend using progressive enhancement
NFR_US_04	Usability	Services must use generic browser capabiities including but not limited to Mircosoft Edge, Microsoft Internet Explorer, Google Chrome, instead of specific capabilities and/or the use of browser plug-ins that prevents people from using the services	Must Have	

NFR_US_05	Usability	All data captured through a user interface must be validated **on entry** and invalid entries rejected by the user interface, with an explanatory reason to the user.	Must Have	
NFR_US_06	Usability	Where relevent, when a **business logic** error on submission occurs the user should receive an explanatory message indicating what they have done wrong.	Must Have	
NFR_US_07	Usability	Where relevent, when a system error occurs the user should receive an explanatory message indicating that there is something wrong with the system which has not been caused by them; the message will explain what action should be taken the user.	Must Have	
NFR_US_08	Usability	The system should be able to utilise colours, logos, text and fonts to reflect HMCTS branding wherever possible.	Should Have	
NFR_US_09	Usability	The platform shall have the capability to extend across different operating systems (such as Windows, MacOS) and device types, such PCs, Laptops, tablets and smartphones.	Must Have	
NFR_US_10	Usability	Solution must be able to switch between Welsh language and English language for all static content and labels.	Should Have	
NFR_US_11	Usability	The solution will not require the installation of an executable on the desktop i.e. the solution will be 'thin client'.	Must Have	

5.1.1.6. HMCTS Security Non-Functional Requirements

HMCTS ID	ISO/IEC 27001:2013 Control Set	Control	NCSC CAF Objective	Purpose	MoSCoW	Primary Evidence	Security Non-functional Requirements
SEC-08-007	Operations Security	Audit, Logging and Monitoring	(C) Detecting Cyber Security Events	BRD	Must	Technical Design Documents	The solution must ensure security log events and audit events are retained and available for a configurable period of time. At a minimum, the solution must ensure security events and audit events (1) are stored and made available for 90 days (2) contain an accurate date and time stamp (3) are verbose enough to support effective security incident management and forensics.

SEC-05-001	Access Control	Authentication	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must implement secure authentication and authorisation mechanisms to reduce the likelihood of unauthorised access to the solution. At a minimum, the solution must support OAuth 2.0, OIDC, SAML2.0 and LDAPS (or equivalent).
SEC-05-002	Access Control	Authentication	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must support or implement Multi-Factor Authentication (MFA). At a minimum, Time-based One-Time Password (TOTP) must be supported.
SEC-05-003	Access Control	Authentication	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	Then solution must support user authentication to existing Identity and Access Management (IdAM) services used by HMCTS. At a minimum, the solution must (1) support Microsoft Entra ID (formerly Azure Active Directory) (2) respond to changes to user accounts or permissions within the HMCTS IdAM, within the minimum time possible (maximum 30 minutes).
SEC-05-007	Access Control	Authentication	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must support Single Sign-On (SSO).
SEC-05-004	Access Control	Authorisation	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must provide the technical capability to configure a robust and granular Role Based Access Control (RBAC) model. At a minimum, the solution must provide the ability to (1) manage user permissions at an individual, team and group level (2) support Just-in-Time (JIT) access (3) enforce the Principle of Least Privilege (PoLP) (4) separate the request and approval stages of account creation (5) log changes to user permissions.
SEC-13-001	Information Security Aspects of Business Continuity Management	BCMS	(D) Minimising The Impact of Cyber Security	Procurement	Must	SMP	The supplier must develop and maintain a Business Continuity and Disaster Recovery Plan that meets the requirements of ISO/IEC22301 (https://www.iso.org/standard/75106.html).

			Incidents				
SEC-08-006	Operations Security	Change Management	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must ensure any changes to hardware and software configurations are performed under formal change control. At a minimum, the supplier must audit against unauthorised changes at least once during any period of twelve months and provide evidence to HMCTS of audit findings.
SEC-11-001	Supplier Relationships	Contracts	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must ensure, and provide evidence to HMCTS, that all security requirements – functional and non-functional – applicable to the solution or service, will flow down in the supply chain and will apply to all sub-contractors, partners, and suppliers that participate in the solution or service.
SEC-06-001	Cryptography	Credentials and Secrets Management	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must provide a secure mechanism to store and retrieve credentials, cryptographic keys and secrets based on NCSC guidance (https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/choosing-and-configuring-a-kms-for-secure-key-management-in-the-cloud). At a minimum, the solution must (1) use a tamper-resistant secure storage (2) provide a mechanism for automated rotation of keys and secrets (3) provide a mechanism for deletion or revocation of cryptographic keys (4) log and monitor access to cryptographic keys.
SEC-14-004	Compliance	Cyber Essentials	(A) Managing Security Risk	Procurement	Must	Certificates	The supplier must hold and maintain Cyber Essentials (CE) Plus certification the scope of which includes the systems within the solution provided to HMCTS.

SEC-04-002	Asset Management	Data Classification	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must implement measures to secure the physical handling, use, storage, transport and disposal of HMCTS information assets (whether in paper or electronic form) in accordance with the Government Security Classification Policy (https://www.gov.uk/government/publications/government-security-classifications) and SMP.
SEC-14-006	Compliance	Data Protection	(A) Managing Security Risk	BRD	Must	Technical Design Documents	The solution must ensure all HMCTS data is stored, supported and processed within the United Kingdom (UK). The HMCTS SIRO must approve any departure from this.
SEC-14-007	Compliance	Data Protection	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must ensure that all aspects of the service provided to HMCTS is performed in accordance with Data Protection Legislation (UK GDPR and UK DPA), comply with both the law and good practice, respect the rights of individuals, be open and honest about how it handles personal data.
SEC-04-003	Asset Management	Decommissioning	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must decommission, dispose, sanitise or destruct infrastructure and data in accordance with National Cyber Security Centre (NCSC) guidance (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media). The supplier must provide a decommissioning approach document, at least 3 months ahead of the first planned decommissioning activity, detailing the decommissioning and disposal methodology for approval by HMCTS.
SEC-14-011	Compliance	Detailed Security Requirements	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must comply with HMCTS Detailed Security Requirements provided with the contract.

SEC-06-002	Cryptography	Encryption (Data at rest)	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must implement cryptographic controls to provide data at rest protection for all HMCTS information assets based on NCSC guidance (https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-2-asset-protection-and-resilience#principle23). At a minimum, the solution must (1) not use NIST deprecated or disallowed ciphers (2) support symmetric algorithm AES (3) support 256-bit key length (4) support AES-GCM or AES-XTS modes of operation (5) support SHA-256 hashing algorithm.
SEC-06-003	Cryptography	Encryption (Data in transit)	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must implement cryptographic controls to provide data in transit protection for all HMCTS information assets based on NCSC guidance (https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data). At a minimum, the solution must (1) not use NIST deprecated ciphers (2) support TLS 1.2 (3) disable TLS features known to be insecure (4) support 2048-bit RSA or ECDSA-256 P-256 Curve signing algorithms (5) support SHA-256 hashing algorithm.
SEC-08-003	Operations Security	End User Devices	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must ensure devices used to access or manage HMCTS data under the management authority of the supplier have a minimum set of security policy configurations enforced. At a minimum, all supplier devices must satisfy the security requirements set out in the NCSC Device Security guidance (https://www.ncsc.gov.uk/collection/device-security-guidance).
SEC-08-004	Operations Security	Environments	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must enforce physical or logical segregation between production and non-production environments.
SEC-14-008	Compliance	HMCTS Audit and Inspection	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must allow for audits and inspections of its data processing activity by HMCTS or an auditor designated by HMCTS.

SEC-14-010	Compliance	Internal audit	(A) Managing Security Risk	Procurement	Should	Reports	The supplier should conduct internal security audits from time to time (and at least annually) across the scope of the ISMS and additionally after any change or amendment to the ISMS or SMP. At a minimum, security audit findings should be shared with HMCTS in the form of a report.
SEC-04-001	Asset Management	Inventory	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must produce and maintain an accurate inventory of information, system, hardware (where applicable) and software assets used to deliver the service.
SEC-14-003	Compliance	ISMS	(A) Managing Security Risk	Procurement	Must	Certificates	The supplier must hold and maintain valid ISO 27001 certification for their Information Security Management System (ISMS). The certification must be issued by a UKAS registered certification body the scope of which fully and explicitly includes the system(s) used for the solution, service and data and all related operations and procedures.
SEC-05-006	Access Control	JML	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	1. The solution must ensure that user accounts for self-service users meet the following requirements: a. Joiners user accounts are automatically created once the person/appointment record meets given criteria. b. User accounts are automatically updated as appropriate when staff transition between teams. c. User accounts remain active for 90 days after the individual's leaving date as recorded on the person record and are automatically deactivated after the 90 day period.
SEC-05-006	Access Control	JML	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	2. The solution must ensure that user accounts for System Administrator & Operational users meet the following requirements: a. Joiners user accounts are validated and enabled by a system administrator. b. Accounts for users transitioning between teams are subject to validation and enablement/disablement by a system administrator. c. User accounts are automatically deactivated for staff who leave the organisation.
SEC-03-003	Human Resource Security	Location	(B) Protecting	Procurement	Must	SMP	The supplier must ensure all personnel (and those within the supply chain) are based in the United Kingdom (UK). The HMCTS SIRO must approve any departure from this.

			Against Cyber Attack				
SEC-08-001	Operations Security	Malware	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must implement malware controls to detect and prevent malware-based attacks. At a minimum, the solution must (1) use up-to-date malware detection signatures or heuristics (2) prevent attacks in near real-time (3) be monitored to ensure malware controls are always enabled (4) meet NCSC pattern for Safely Importing Data (https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data) for any function designed to ingest, upload or store data from an untrusted source.
SEC-10-006	System Acquisition, Development, and Maintenance	NCSC CAF	(B) Protecting Against Cyber Attack	Procurement	Should	SMP	The supplier should share security related information about the solution in order to assist HMCTS in completing the NCSC Cyber Assessment Framework (CAF)(https://www.ncsc.gov.uk/collection/caf)
SEC-10-005	System Acquisition, Development, and Maintenance	NCSC CSP	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must meet all applicable requirements of the NCSC Cloud Security Principles (https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles). At a minimum, all mutli-tenant cloud services must demonstrate how tenant separation or boundaries are implemented within compute, storage and data flows and networking.
SEC-10-007	System Acquisition, Development, and Maintenance	NCSC SDP	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must demonstrate implementation of the NCSC Secure Design Principles (https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles).
SEC-09-001	Communications Security	Network Security	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must implement network security controls to make a network compromise difficult or reduce the impact of any network-based attack. At a minimum, controls should include (1) limiting all inbound and outbound traffic to only those sources/destinations and protocols required for the solution to function (2) network segmentation or zones (3) preventing lateral movement based on NCSC Preventing Lateral Movement Guidance

							(https://www.ncsc.gov.uk/guidance/preventing-lateral-movement) (4) preventing Denial-of-Service (DoS) attacks.
SEC-10-008	System Acquisition, Development, and Maintenance	OWASP	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must ensure any web applications and APIs are designed and implemented to prevent common security attacks such as those listed in the OWASP Top 10 (https://owasp.org/www-project-top-ten/).
SEC-07-001	Physical and Environmental Security	Physical and Environmental Security	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must implement physical security controls at locations used in the provision of the solution and service. At a minimum, National Protective Security Authority (NPSA) guidance (https://www.npsa.gov.uk/advice-guidance) must be consulted to identify proportionate controls for preventing unauthorised physical access, damage and interference to information processing facilities where HMCTS data may be stored, processed and managed from.
SEC-01-001	Information Security Policies	Policy	(A) Managing Security Risk	BRD	Should	Technical Design Documents	The solution should comply with applicable HMCTS Security Policies (https://tools.hmcts.net/confluence/display/ISMS/Policy+Areas).
SEC-01-002	Information Security Policies	Policy	(A) Managing Security Risk	Procurement	Should	SMP	The supplier should comply with applicable HMCTS Security Policies (https://tools.hmcts.net/confluence/display/ISMS/Policy+Areas)
SEC-05-005	Access Control	Privileged Access	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must ensure segregation of duties by privileged users of the services. At a minimum this must include (1) ensuring the Principle of Least Privilege (PoLP) is always applied (2) ensuring separation of request and approval for account creation (3) logging changes to user permissions (4) regularly reviewing privileged user access.

SEC-12-001	Information Security Incident Management	Process	(D) Minimising The Impact of Cyber Security Incidents	Procurement	Must	SMP	The supplier and HMCTS must notify the other upon becoming aware of any security incident, breach of security or any potential or attempted breach of security (including throughout the supply chain) in accordance with the ISMS, SMP and HMCTS Security Incident Management Policy (https://tools.hmcts.net/confluence/display/ISMS/Security+Incident+Management).
SEC-10-001	System Acquisition, Development, and Maintenance	Risk Assessments	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must produce and maintain an information security risk assessment of the solution based on a formal risk assessment methodology and share the output with HMCTS in the form of a documented information security risk register. At a minimum the risk assessment must include (1) risk events (2) risk causes (3) risk impact (4) risk severity (5) mitigating controls
SEC-14-002	Compliance	SAL	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must ensure that all changes to services impacting IT security are approved in accordance with the agreed change procedure and take account of the latest Security Aspects Letter (SAL)(https://tools.hmcts.net/confluence/display/ISMS/SAL+Template).
SEC-10-004	System Acquisition, Development, and Maintenance	Secure Configuration	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution components must be deployed and configured in accordance with any published and applicable secure deployment or configuration guides made available by Vendors, NCSC or Center for Internet Security (CIS). For example: Microsoft Cloud Security Benchmark (https://learn.microsoft.com/en-us/security/benchmark/azure/) AWS Security Documentation (https://docs.aws.amazon.com/security/) NCSC Device Security Guidance for Windows (https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/windows) CIS Benchmark for RHEL (https://www.cisecurity.org/benchmark/red_hat_linux)
SEC-08-008	Operations Security	Security Monitoring	(C) Detecting Cyber Security Events	BRD	Must	Technical Design Documents	The supplier must ensure the solution is under 24x7x365 security monitoring to detect suspicious and unauthorised activities based on NCSC Security Monitoring guidance (https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf)

SEC-08-009	Operations Security	Security Monitoring	(C) Detecting Cyber Security Events	BRD	Should	Technical Design Documents	The supplier should provide an automated mechanism to export security event logs to HMCTS security monitoring systems.
SEC-14-001	Compliance	SMP	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must prepare, develop, maintain and deliver HMCTS for approval a complete and up to date Security Management Plan (SMP) covering all services delivered under contract. At a minimum, the SMP must (1) be structured in accordance with the HMCTS SMP template (https://tools.hmcts.net/confluence/display/ISMS/SMP+Template) (2) identify how the supplier's ISMS applies to the services offered to HMCTS (3) explicitly detail how security non-functional requirements and outcomes are being implemented or met (4) identify the necessary delegated organisational roles defined for those responsible for delivering and overseeing the SMP (5) detail the supplier approach and processes for delivering the services using Sub-Contractors and third parties authorised by HMCTS.
SEC-02-001	Organisation of Information Security	SPOC	(A) Managing Security Risk	Procurement	Must	SMP	The supplier must provide HMCTS with a Single Point Of Contact (SPOC) to act as coordinator and focal point for all the security aspects to the service and the SPOC (or a delegate) must be available to attend regular security working group meetings with HMCTS.
SEC-08-005	Operations Security	SyOPs	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must not extract/export any HMCTS data outside of the service, without written consent from HMCTS. Any HMCTS approved extract/export must be strictly controlled and recorded.
SEC-08-012	Operations Security	SyOPs	(B) Protecting Against Cyber Attack	Procurement	Should	SMP	The supplier should comply with any Security Operating Procedures (SyOPs) that have been issued to HMCTS by organisations for which HMCTS processes data. At a minimum, this will include SyOPs from (1) Home Office (2) MoJ (3) Judiciary

SEC-10-002	System Acquisition, Development, and Maintenance	System Interfaces	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must ensure any system-to-system data flows or Application Programming Interfaces (APIs) are protected using good practice security controls. At a minimum controls should include (1) authentication (2) integrity checking (3) encryption (4) limited data exposure (5) ensuring all third-party interfaces are covered by any MoU or other type of agreement.
SEC-10-003	System Acquisition, Development, and Maintenance	Technical Design Documentation	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution technical design documents issued to HMCTS must explicitly detail how HMCTS technical security non-functional requirements and outcomes are being implemented or met. At a minimum, all technical design documents must (1) include a dedicated security section (2) highlight any shortcomings against HMCTS technical security non-functional requirements (3) highlight any single point of failure that could impact the availability of the solution.
SEC-08-010	Operations Security	Technical Vulnerability Management	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must perform regular vulnerability scanning of all the components within the solution. At a minimum, the scope must include (1) devices (2) infrastructure (3) software (4) firmware (5) software dependencies (6) application code analysis (SAST and DAST).
SEC-08-011	Operations Security	Technical Vulnerability Management	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must remediate all vulnerabilities in accordance with the HMCTS Vulnerability Management Policy (https://tools.hmcts.net/confluence/display/ISMS/Vulnerability+Management). At a minimum CRITICAL severity vulnerabilities must be remediated as soon as reasonably practical (take first priority) and HIGH severity vulnerabilities remediated within 7 days.
SEC-08-013	Operations Security	Technical Vulnerability Management	(B) Protecting Against Cyber Attack	Procurement	Should	Reports	The supplier should provide regular reporting on vulnerability management. At a minimum, this must include information relating to (1) vulnerabilities detected (2) exploitability (3) mitigating controls (4) recommendations for remediation (4) remediation progress.

SEC-14-005	Compliance	Technical Vulnerability Management	(B) Protecting Against Cyber Attack	Procurement	Must	Reports	The supplier must perform an IT Health Check (ITHC) of the solution under the CHECK scheme (https://www.ncsc.gov.uk/information/check-penetration-testing). At a minimum, this must include (1) performing an ITHC within the last six months of service commencement, thereafter annually and upon significant change to the system (or a system component) (2) a scope that contains all components within the solution or a subset that has been approved by HMCTS (3) sharing ITHC report findings with HMCTS (4) remediation of all discovered vulnerabilities in accordance with the HMCTS Vulnerability Policy (https://tools.hmcts.net/confluence/display/ISMS/Vulnerability+Management)
SEC-10-009	System Acquisition, Development, and Maintenance	Test Data	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The solution must ensure live HMCTS data (or copies of) are only stored in production (operational) systems.
SEC-13-002	Information Security Aspects of Business Continuity Management	Testing backups	(D) Minimising The Impact of Cyber Security Incidents	Procurement	Must	SMP	The supplier must test backup solutions. At a minimum this must include (1) a backup test at least every three months (2) verifying data reliability and integrity of data in scope of the ISMS (3) ensuring that any testing meets the requirements of the BCDR plan (4) verifying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) can be met.
SEC-03-004	Human Resource Security	Training & Awareness	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must ensure that all supplier and sub-contractor staff who have access to personal data, including staff in their supply chain if appropriate, undergo a session of data protection and information risk awareness training on induction and annually thereafter.
SEC-08-002	Operations Security	Vendor Support	(B) Protecting Against Cyber Attack	BRD	Must	Technical Design Documents	The supplier must ensure all software and hardware is supported by a vendor that produces regular security updates. At a minimum, the supplier must (1) inform HMCTS six months in advance of software or hardware reaching end of vendor support (2) inform HMCTS if extended support agreements have been purchased to obtain security updates.

SEC-03-001	Human Resource Security	Vetting and Clearance	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must perform appropriate checks on all personnel involved in the design, delivery and operation of the solution (pre-employment, during employment, termination and change of employment) in order to ensure the security of HMCTS information assets and the safety of staff and individuals within HMCTS. At a minimum, personnel must successfully complete Baseline Personnel Security Standard (BPSS)(or equivalent) pre-employment screening before being granted access to HMCTS information assets (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard).
SEC-03-002	Human Resource Security	Vetting and Clearance	(B) Protecting Against Cyber Attack	Procurement	Must	SMP	The supplier must ensure all personnel (and those within the supply chain) hold the relevant vetting and clearance in accordance with the HMCTS Vetting and Clearance Policy (https://tools.hmcts.net/confluence/display/ISMS/Vetting+and+Clearance). The HMCTS SIRO must approve any departure from this. At a minimum, all personnel with access to (1) bulk personal data or administrative privileges will require Security Check (SC) clearance (2) Home Office or Policing systems will require Non-Police Personnel Vetting (NPPV) Clearance.

Contractual Framework	Clause	Wording
G-Cloud 13	[4.1.a]	the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
G-Cloud 13	[4.2]	The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.
G-Cloud 13	[13.4]	The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
G-Cloud 13	[13.6.3]	the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection
G-Cloud 13	[13.6]	The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with: 13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy: https:/www.gov.uk/government/publications/government-securityclassifications

G-Cloud 13	[16.1]	If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
G-Cloud 13	[16.2]	The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
G-Cloud 13	[16.3]	If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
G-Cloud 13	[16.4]	Responsibility for costs will be at the: 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
G-Cloud 13	[16.7]	If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date
G-Cloud 13	[19.5.4]	destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
G-Cloud 13	[2.1.g.iii]	have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;
G-Cloud 13	[4.1.5]	complete any necessary Supplier Staff vetting as specified by the Buyer
NS3	[1.1.1]	securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
NS3	[1.1.2]	securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.
NS3	[1.1]	The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.
NS3	[2.x]	End user devices
NS3	[3.1]	The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.
NS3	[3.4.3.d]	where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
NS3	[3.4.5]	document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier

		becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and
NS3	[3.x]	Information Security Management System (ISMS)
NS3	[4.x]	Security Management Plan
NS3	[6.2]	The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.
NS3	Annex1[6.3]	The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
NS3	LFSR[6.3]	Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
NS3	[6.4]	All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
NS3	[6.x]	Security of Supplier Staff
NS3	[9.x]	Vulnerabilities and fixing them

Data Migration Outline
Provides information on data sets to be migrated to the new system.

The following items relate to the transaction data proposed for migration:
Only fee and expense data for the current financial year is required for correct calculations to be completed in the system.
Claims can be made by JOH for sittings in the previous financial year, so migrating records for the full previous financial year could also be considered.
In order for fee and expense data for the current financial year to be complete, associated person, appointment, and reference data will be required.

Data Name	Data Description	Current Source	Future Source	Format	Purpose	Migrate Active	Migrate Historical	Migration Destination	Retention Requirements	Regulation	Volume	Notes

Name of Data item/Structure	*Further information about the Data*	*Where is it currently? Excel? Current System?*	*Where will it be sourced once the JFEPS replacement solution is in place?*	*Current Format: csv, txt, sql…*	*As referred by Gary, why we need to migrate the data: due to retention policy? To Allow computations/ functions in JFEPS? To make reports from new JFEPS?*				*Retention Time as mandated by policy or functional requirements*	*Reference to regulation for retention time*	*Approximate number of records to migrate*	*Points to consider in relation to this Data set*
HR Data	JOH Person & Appointment Data: Personal Code, Name, NI Number, D.o.B, Address, Appointments etc.	JFEPS	Judicial HR (eLinks)	db	Core data for process requirements	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		9,000	JO presumably has to retain the master of this data for the designated retention period, so does JPET also need to retain it? Will need to retain

												sufficient minimal information to link fee/expense payment records to.
Bank Details	JOH Bank Account details: Account Number, Sort Code, Account Name etc.	JFEPS	JFEPS	db	Core data for process requirements	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	7 years after retirement		9,000	Retention schedule specifies bank details must be kept until 7 years after retirement.
Pension Enrolment	JOH Pension Scheme membership: Scheme Name, Enrolment Date, Opted Out etc.	Unknown	JFEPS (TBC)	Unknown	Will be required to align with Pension Ops plans	TBC	TBC	JFEPS Replacement	Until Judge is 110		9,000	Pension Ops presumably has to retain the master of this data for the designated retention period, so does JPET also need to retain it? Can this

												migration wait until Pension Ops have their bit lined up?
Courts Fees	Fees for Court sittings: Payroll ID, Name, Cost Centre, Activity, Date, Session Length, Fee Amount, Analysis Code	Excel	OPT	Excel (could be xlsx or csv)	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		4,000 for each full month migrated	Not currently processed through JFEPS, so will need to compile data from multiple spreadsheets. Alternative may be to request data from Payroll Provider.
Mental Health Fees	Fees for Mental Health Tribunal: Payroll ID, Name, Role, Cost Centre, Start Date, End Date, Session	JFEPS & Excel	MARTHA	db; Excel	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		3,500 for each full month migrated	

	Length, Fee Amount, Analysis Code											
Asylum Support Fees	Fees for Aylum Support Tribunal: Fee Type, Email, Date, Notes, Location	JFEPS	ARIA	db	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		15 for each full month migrated	
SEND Fees	Fees for Special Education Needs & Disabilities Tribunal: Name, NI Number, Datem Session Length, Location, Account Code, Fee Amount	JFEPS	GAPS/List Assist	db	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		1,000 for each full month migrated	
Training Fees	Fees for Training Course attendance: Payroll ID, Name, Email,	JFEPS	Judicial HR (eLinks) (TBC)	db	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		2,000 for each full month migrated	

	Member Type, Cost Centre, Attendance Type, Date, Session Length, Fee Amount, Analysis Code											
SSCS Fees	Fees for Social Security & Child Support Tribunal: Name, ID number, NI Number, Role, Date, Session Length, Region, Location, Cost Centre, Account Code, Fee Amount	Excel	GAPS/List Assist	Excel (could be xlsx or csv)	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		7,500 for each full month migrated	Not currently processed through JFEPS, so will need to compile data from multiple spreadsheets. Alternative may be to request data from Payroll Provider.

Other Fees	Manually claimed fees entered directly into JFEPS - self-service + manual input by JPET from hard-copy forms: data items TBC	JFEPS	JFEPS	db	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		8,500 for each full month migrated	
Expenses	Manually claimed expenses entered directly into JFEPS - self-service + manual input by JPET from hard-copy forms: data items TBC	JFEPS	JFEPS	db	Core payments data	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		24,000 for each full month migrated	

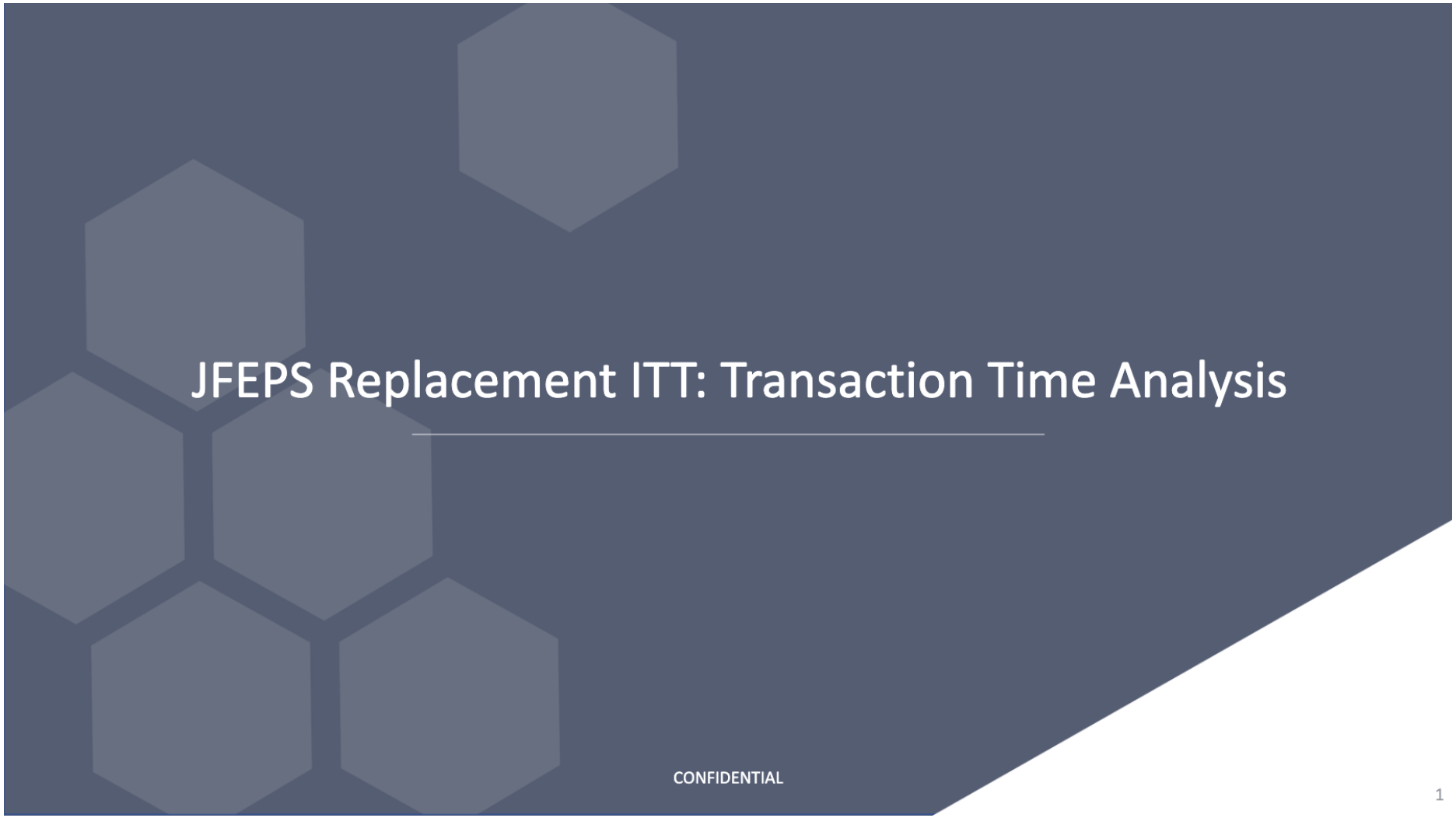
Attached Documents	Uploaded documents linked to fee and expense claims: pdf, jpg, png, msg etc	JFEPS	JFEPS	TBC	Evidence to support fee and expense claims	All	Current financial year	JFEPS Replacement	Until Judge is 110		24,000 for each full month migrated, assuming 1 document per expense claim	Not necessarily required for payments that have already been processed. Feasibility will depend on how these documents are held in the current database and how they will be held in the new database. Physical files will be more difficult to migrate than BLOBs.

Pension Payments	Payments made into Pension Schemes on behalf of JOH based on pensionable pay & scheme membership: data items TBC	Unknown	Unknown	Unknown	Current & historical pension contribution records	All	Current financial year	JFEPS Replacement. Data beyond current financial year TBC	Until Judge is 110		6,000	Unsure where this is currently held. If not in JFEPS do we need to migrate?
Fee Types	Fee Types & associated attributes: Name, Active, Group, Entry Type, Nominal Code, Approval Route, Limit Amount, Limit Type, Effective Date, Rate, Historical Effective Dates,	JFEPS	JFEPS	db	Fee payment calculation & validation	All	Current financial year	JFEPS Replacement	Until associated payment data retention period has expired		1,300	Reference Data. Only need to migrate as much as is required to define migrated data correctly and support future data.

	Historical Rates											
Expense Types	Expense Types & associated attributes: Name, Active, Group, Entry Type, Nominal Code, Approval Route, Limit Amount, Limit Type, Effective Date, Rate, Historical Effective Dates, Historical Rates	JFEPS	JFEPS	db	Fee payment calculation & validation	All	Current financial year	JFEPS Replacement	Until associated payment data retention period has expired		140	
Cost Centre Codes	Cost Centre Codes & associated	JFEPS	TBC	db	Cost allocation	All	Current financial year	JFEPS Replacement	Until associated payment data		2,000	

	attributes: data items TBC								retention period has expired			
Account Codes	Account Codes & associated attributes: data items TBC	JFEPS	TBC	db	Cost allocation	All	Current financial year	JFEPS Replacement	Until associated payment data retention period has expired		200 Pay Element IDs and Account Codes align in current system	
Pay Elements	Pay Elements & associated attributes: data items TBC	JFEPS	TBC	db	Cost allocation	All	Current financial year	JFEPS Replacement	Until associated payment data retention period has expired		200 Pay Element IDs and Account Codes align in current system	
Locations	Locations & associated attributes: data items TBC	JFEPS	MRD	db	London Weighting calculation	All	Current financial year	JFEPS Replacement	Until associated payment data retention period has expired		1,000	

ITT Transaction Time Analysis


JFEPS Replacement ITT: Transaction Time Analysis
CONFIDENTIAL
1

Document Control

Document Purpose
Provides a heatmap and chart to show the volume of Fee and Expense Claim submissions in the current system over a six month period.

ITT: Transaction Time Heatmap

Time/Day Analysis	Day of Week							
Time Bucket	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Grand Total
00:00-01:00	124	63	131	80	161	82	28	669
01:00-02:00	52	33	72	16	48	30	13	264
02:00-03:00	36	24	47	4	11	13	5	140
03:00-04:00	28	20	28	3	37	4		120
04:00-05:00	29	17	42	38	75	26	18	245
05:00-06:00	38	30	60	92	84	21	26	351
06:00-07:00	125	200	177	284	287	149	150	1,372
07:00-08:00	517	590	550	722	748	341	242	3,710
08:00-09:00	1,318	1,261	1,196	1,329	1,671	621	436	7,832
09:00-10:00	2,157	1,974	2,318	2,114	2,872	923	663	13,021
10:00-11:00	2,496	2,364	2,797	2,513	3,249	1,144	1,074	15,637
11:00-12:00	2,933	2,844	4,047	2,445	3,142	1,162	1,017	17,590
12:00-13:00	2,715	5,885	3,357	2,572	3,394	1,131	1,079	20,133
13:00-14:00	2,556	2,389	4,875	2,648	2,791	960	848	17,067
14:00-15:00	2,555	3,208	3,223	5,706	5,203	1,079	1,141	22,115
15:00-16:00	3,046	3,434	3,469	10,132	9,282	1,066	827	31,256
16:00-17:00	2,879	2,565	5,473	5,133	3,018	978	952	20,998
17:00-18:00	3,206	1,969	4,785	3,199	2,500	795	1,242	17,696
18:00-19:00	2,492	1,596	1,908	2,019	1,775	955	1,086	11,831
19:00-20:00	1,382	1,171	1,265	1,419	1,288	537	827	7,889
20:00-21:00	1,134	1,023	1,059	999	1,029	497	620	6,361
21:00-22:00	777	875	850	780	808	356	634	5,080
22:00-23:00	441	645	803	599	597	177	582	3,844
23:00-00:00	315	264	300	297	374	126	281	1,957
Grand Total	**33,351**	**34,444**	**42,832**	**45,143**	**44,444**	**13,173**	**13,791**	**227,178**

This heatmap is a visual representation of the days and times that Fee and Expense Claims are submitted.

The data is taken from a report of all Fee and Expense Claims submitted in the existing JFEPS system in the six months between 10 September 2023 and 9 March 2024.

The heatmap shows that the peak times for Fee and Expense Claim submission are between 14:00 and 16:00 on Thursday and Friday, but that submissions are made at nearly all times of day.

It is important to note that not all Fees are currently processed through the JFEPS system. Approximately 11,000 Fee Claims each month (for Courts and SSCS) are processed outside the system.

The chart on the following page is a representation of the same data set showing the number of transactions per hour, with a line for each day of the week.

ITT: Transaction Time Graph