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

Part A: Further Competition Order Form

CALL-OFF REFERENCE:	Project_9428 / itt_3369 / con_26762
THE BUYER:	The Secretary of State for Education ("Department for Education")
BUYER ADDRESS:	Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
SUPPLIER REFERENCE:	BTMVDS01662
THE SUPPLIER:	BRITISH TELECOMMUNICATIONS PLC
SUPPLIER ADDRESS:	1 Braham Street, LONDON, E1 8EE
REGISTRATION NUMBER:	01800000
DUNS NUMBER:	22 701 5716
SID4GOV ID:	22 701 5716

APPLICABLE FRAMEWORK CONTRACT:

This Order Form is for the provision of the Call-Off Deliverables and dated 21st March 2025.

It's issued under the Framework Contract with the reference number RM6261 for the provision of Mobile Voice and Data Services.

CALL-OFF LOT(S):

Lot 2: Mobile Voice and Data Solutions.

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) RM6261.
3. Framework Special Terms.
4. The following Schedules in equal order of precedence:
    - Joint Schedules for RM6261
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 10 (Rectification Plan)

    - Joint Schedule 11 (Processing Data)
    - Joint Schedule 12 (Supply Chain Visibility)
- Call-Off Schedules for RM6261
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 2 (Staff Transfer) – Schedule wording has not been included in the body of this Call-Off Contract; however, the Parties acknowledge that it shall form part of the Contract, and all provisions will be incorporated as such. For the avoidance of doubt, as there will be no transfer of staff on entry, Parts C and E of the Schedule shall apply to this Call-Off Contract.
    - Call-Off Schedule 3 (Continuous Improvement)
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 6 (ICT Services)
    - Call-Off Schedule 7 (Key Supplier Staff)
    - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
    - Call-Off Schedule 9 (Security)
    - Call-Off Schedule 11 (Installation Works)
    - 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 20 (Call-Off Specification)
    - Call-Off Schedule 24 (Supplier Furnished terms)
5. CCS Core Terms (version 3.0.11).
6. Joint Schedule 5 (Corporate Social Responsibility) RM6261.
7. 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:

- Special Term 1 – Appendix A: Departmental Security Standards shall be incorporated into the Contract as the Buyer's Security Policy.
- Special Term 2 – 'Part B – Testing' of Call-Off Schedule 13 (Implementation Plan and Testing) will be deleted in its entirety, and shall not apply to this Contract. The Services shall be deemed as successfully implemented once:
    - eSIMs have been deployed to all applicable End Users;
    - phone numbers have been ported from the incumbent supplier for all End Users; and,
    - all End Users have been transitioned to the Supplier's Mobile Voice and Data Solution.

CALL-OFF START DATE:	1st April 2025
CALL-OFF EXPIRY DATE:	31st May 2028
CALL-OFF INITIAL PERIOD:	3 Years, 2 Months
CALL-OFF OPTIONAL EXTENSION PERIOD:	12 Months

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION:
90 days.

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

MAXIMUM LIABILITY:
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£[redacted]exc. VAT**.

CALL-OFF CHARGES:
Total Call-Off Charges: **£173,124 exc. VAT**.

See further 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).

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law; and,
- Benchmarking using Call-Off Schedule 16 (Benchmarking).

REIMBURSABLE EXPENSES:
None.

PAYMENT METHOD:
Electronic payment via BACS.

BUYER'S INVOICE ADDRESS:
Invoices to be sent electronically to AccountsPayable.OCR@education.gov.uk. All invoices must include a valid Purchase Order number.

A copy of all invoices must also be sent to [redacted](Service Manager).

BUYER'S AUTHORISED REPRESENTATIVE:

[redacted]Piccadilly Gate, Store Street, Manchester, M1 2WD

BUYER'S ENVIRONMENTAL POLICY: (for information only)
The Supplier must adhere to the Greening government: ICT and digital services strategy 2020-2025 in its delivery of the Services.

SECURITY REQUIREMENTS:
In accordance with Call-Off Schedule 9, Part A (Short Form Security Requirements) applies.

BUYER'S SECURITY POLICY:
See Special Term 1 – Departmental Security Standards.

SUPPLIER'S AUTHORISED REPRESENTATIVE:
[redacted]
3 Snowhill, Snowhill Queensway, BIRMINGHAM, B4 6GA

SUPPLIER'S CONTRACT MANAGER:
[redacted]
One Braham
Braham Street
London
E1 8EE

PROGRESS REPORT FREQUENCY:
See details in Call-Off Schedule 1 (Transparency Reports).

PROGRESS MEETING FREQUENCY:
See details in Call-Off Schedule 15 (Call-Off Contract Management).

KEY STAFF:

Key Role	Key Staff	Contact Details
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

KEY SUBCONTRACTOR(S):

The Supplier may subcontract the Service to EE Limited ("**EE**") and will assign the benefit of Order to EE in respect of ordering, provision, maintenance, invoicing, and payment for the Service.

Key Sub- contractor name and address (if not the same as the registered office)	**Registered office and company number**	**Related product/Service description**	**Key role in delivery of the Services**
EE Limited	1 Braham Street, London, E1 8EE	Mobile Voice and Data provider, Service Provider	Primary Voice and Data Service provider

COMMERCIALLY SENSITIVE INFORMATION:

See details in Joint Schedule 4 (Commercially Sensitive Information).

SERVICE CREDITS:

Service Credits will accrue in accordance with Call-Off Schedule 14 (Service Levels).

The Service Credit Cap is: 5% of the Total Call-Off Charges.

The Service Period is: Monthly.

A Critical Service Level Failure is: consistent failure to meet two (2) or more Service Levels for more than four (4) consecutive Months.

ADDITIONAL INSURANCES:

Not applicable.

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), and meet the agreed social value KPI outlined at Annex 1 to Part A: Short Form Service Levels Table of Call-Off Schedule 14 (Service Levels).

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:	01/05/25	**Date:**	01/05/25

Joint Schedule 1 (Definitions)

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 Central Government 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;

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

1.3.13 any reference in a Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

(a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and

(b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.14 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.3.15 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

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;
"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) where the Relevant Authority is a Buyer, and the value of the relevant Call-Off Contract is greater than £3million, verify the Open Book Data; d) verify the Supplier’s and each Subcontractor’s compliance with the Contract and 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"	means: a) the Relevant Authority's internal and external auditors; b) the Relevant Authority'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 Relevant Authority 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;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Business Hours"	standard business hours from 0800 to 1800 Monday to Friday, excluding bank holidays
"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 scheduled 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 Award Procedure);
"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);
"Catalogue"	the Supplier's catalogue of Deliverables available to Buyers in relation to Lot 1 only to order without Further Competition;
"Catalogue Publication Portal"	the CCS online publication channel via which Buyers can view the Catalogue;
"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"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;
"Contract Period"	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the: a) applicable Start Date; or b) the Effective Date up to and including 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 UK GDPR;
"Core Network"	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call-Off Contract;
"Core Terms"	CCS' terms and conditions for common goods and services which govern how Suppliers 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: a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work 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) workplace accommodation; (viii) workplace 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; 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; 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 Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but excluding: (i) Overhead; (ii) financing or similar costs; (iii) 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; (iv) taxation; (v) fines and penalties; (vi) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and (vii) non-cash items (including depreciation, amortisation, impairments and movements in provisions);
"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 UK GDPR 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 UK GDPR;
"Data Subject"	has the meaning given to it in the UK 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;
“Direct Award Criteria”	the award criteria to be applied for the direct award of Call-Off Contracts following the process set out in Framework Schedule 7(Cal-Off Award Procedure);
"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 (whether contractual or non-contractual) arising 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: 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 is required by the Supplier in order to provide the Deliverables; and/or 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: the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or 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;
"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;
“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;
“Exempt Buyer”	a public sector purchaser that is: a) eligible to use the Framework Contract; and

	b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of: i) the Regulations; ii) the Concession Contracts Regulations 2016 (SI 2016/273); iii) the Utilities Contracts Regulations 2016 (SI 2016/274); iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848); v) the Remedies Directive (2007/66/EC); vi) Directive 2014/23/EU of the European Parliament and Council; vii) Directive 2014/24/EU of the European Parliament and Council; viii) Directive 2014/25/EU of the European Parliament and Council; or ix) Directive 2009/81/EC of the European Parliament and Council;
"Exempt Call-off Contract"	the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;
"Exempt Procurement Amendments"	any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;
"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;

"FOIA"	the Freedom of Information Act 2000 (as amended from time to time) 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 outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including: a) riots, civil commotion, war or armed conflict; c) acts of terrorism; d) acts of government, local government or regulatory bodies; e) fire, flood, storm or earthquake or other natural disaster, but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;
"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 notice published on the Find a Tender Service;
"Framework Contract Period"	the period from the Framework Start Date until the End Date of the Framework Contract;
"Framework Expiry Date"	the scheduled 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 period of the Framework Contract as specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Contract Period may be extended as 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);
"Further Competition Procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
"UK GDPR"	the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"General Anti-Abuse Rule"	a) the legislation in Part 5 of the Finance Act 2013 and; and b) 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 Tax 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: a) are supplied to the Supplier by or on behalf of the Authority; or b) the Supplier is required to generate, process, store or transmit pursuant to a Contract;
"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 Environment"	The ICT systems used in the delivery of the Services as described in Call-Off Schedule 6 (ICT Services);
"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;
"ICT Services"	The ICT related Services to be delivered under a Call-Off Contract as described in Call-Off Schedule 6 (ICT Services);
"Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:

	a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; c) details of the cost of implementing the proposed Variation; d) 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; e) a timetable for the implementation, together with any proposals for the testing of the Variation; and f) 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;
"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"	with respect to any person, means: a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or: (i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or (ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986; b) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person; c) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person; d) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days; e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business; f) where that person is a company, a LLP or a partnership: (i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other

	companies or the solvent reconstruction of that person; (ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person; (iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or (iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;
"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"	a) 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; b) 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 c) 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 income 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;
"Key Staff"	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: a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or d) 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 e) 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;
"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,

	judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, 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;
"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);
"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: a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or c) 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 Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
"New IPR"	a) 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 b) 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; c) but shall not include the Supplier's Existing IPR;
"Occasion of Tax Non–Compliance"	where: a) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: b) 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; c) 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 d) 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:

	a) 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; e) 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) staff costs 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 grade; iii) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and iv) Reimbursable Expenses, if allowed under the Order Form; f) Overheads; g) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; h) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; i) 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; j) 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 k) the actual Costs profile for each Service Period;
"Operational Hours"	24 hours a day, 7 days a week, 365 days out of the year, less any down time in the case of the self service portal
"Optional Services"	means those services set out in Call-Off Schedule 20 which describe the optional Services which the Buyer may require the Supplier to perform in accordance with Clause 24.9;

"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 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 UK GDPR;
"Personal Data Breach"	has the meaning given to it in the UK 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 UK GDPR;
"Processor"	has the meaning given to it in the UK GDPR;
"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"	a) 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; b) 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 c) committing any offence: iii) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or iv) under legislation or common law concerning fraudulent acts; or v) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or b) 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 Scheme), 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) which shall include: a) full details of the Default that has occurred, including a root cause analysis; d) the actual or anticipated effect of the Default; and e) 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 10.3.1 to 10.3.4 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 as updated from time to time (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: a) 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 f) 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"	a) 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); b) 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 10.5 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;
"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;
"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 Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
“Service Offer”	a Deliverable made available to Buyers by the Supplier via the Catalogue;
“Service Offer Effective Date”	the date when the Service Offer will be available to Buyers on the Catalogue;

“Service Offer Expiry Date”	the date the Service Offer will be/was removed from the Catalogue;
“Service Offer Price Card”	means a list of prices, rates and other amounts for a specific Service Offer;
“Service Offer Template”	the template set out at Annex 1 to Part B of Framework Schedule 3 (Framework Prices);
"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: the Deliverables are (or are to be) provided; or b) 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;
"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:

	a) 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; standards detailed in the specification in Schedule 1 (Specification); standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; 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;
"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); provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or 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's Confidential Information"	a) 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; b) 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; c) 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: a) Achieve a Milestone by its Milestone Date; d) provide the Goods and/or Services in accordance with the Service Levels ; and/or e) 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 Prospectus"	means the written description of the Supplier's functionality of the Deliverables and Supplier Staff and in the format as notified by the Authority to the Supplier, as the same may be amended or updated from time to time
"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;
"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;
"TEM Provider"	means a Supplier appointed by CCS to provide telecoms expense management;
"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 from their requirements as set out in a Call-Off Contract;
"Test Plan"	a plan: a) for the Testing of the Deliverables; and b) setting out other agreed criteria related to the achievement of Milestones;
"Tests "	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" and "Testing" 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;
"Time and Materials"	A pricing mechanism whereby the Buyer agrees to pay the Supplier based upon the work performed by the Supplier's employees and Sub-Contractors, and for materials used in the project, no matter how much work is required to complete the project;
"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 – a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and b) 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"	any change to a 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;
"Volume Discount(s)"	the discounted price(s) applicable to purchases which exceed a Volume Discount Threshold;
"Volume Discount Threshold"	has the meaning set out in paragraph 7 of Framework Schedule 3;
"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) applies in respect of the Deliverables;
"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"	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 of the Core Terms (Changing the Contract).

Contract Details		
This variation is between:	("**the Buyer**") *And* ("**the Supplier**")	
Contract name:	(the contract)	
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	[**insert** proposal]	
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: • **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 the 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 Buyer:

Signature:	
Name:	
Role:	
Date:	

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

Signature:	
Name:	
Role:	
Date:	

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 affecting 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 cooperate 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

The Supplier shall hold the following standard insurance cover from the Framework Start Date in accordance with this Schedule:

professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);

public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);

product liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000); and

employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

What is Commercially Sensitive Information?

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.

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).

Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 of the Core Terms (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:

No.	Date	Item(s)	Duration of Confidentiality
1	From the Call-Off Start Date	Breakdown of Supplier Pricing (i.e. Supplier costs, applicable discounts, etc). This shall exclude the Maximum Total Contract Value which will be disclosed in the Contract's Finder Award Notice to comply with the UK Government's transparency agenda.	Duration of the Call-Off Contract + 5-Years
2	From the Call-Off Start Date	Supplier's Call-Off Tender Submission (as detailed within Call-Off Schedule 4).	Indefinitely
3	From the Call-Off Start Date	Sensitive Personnel Details / Supplier Personal Data	Indefinitely

Joint Schedule 5 (Corporate Social Responsibility)

Part A

Definitions

"Corporate Social Responsibility Reports"	written reports which the Supplier must complete and provide to the Buyer in accordance with Part B of this Schedule;
"Carbon Reduction Plan"	a plan which contains the details of emissions across a single year against a range of emissions sources and greenhouse gases, as per PPN 06/21;
"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;
"Prohibited Items"	means those items set out in Table A which the Supplier must not use in its performance of the Contract; and
"Waste Hierarchy"	means prioritisation of waste management in the following order of preference: (a) prevention – by using less material in design and manufacture. Keeping products for longer; (b) preparing for re-use – by checking, cleaning, repairing, refurbishing, whole items or spare parts; (c) recycling – by turning waste into a new substance or produce, including composting if it meets quality protocols; (d) other recovery – through anaerobic digestion, incineration with energy recovery, gasification and pyrolysis which produce energy (fuels, heat and power) and materials from waste; some backfilling; and (e) disposal - Landfill and incineration without energy recovery.

1. What we expect from our Suppliers

1.1 In February 2019, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work

with the government.
(*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.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 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

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 employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.3 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;

4.1.4 record all disciplinary measures taken against Supplier Staff; and

4.1.5 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.

5.2 The total hours worked in any seven day period shall not exceed 60 hours except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

5.3.1 this is allowed by national law;

5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and

5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 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.

6. Environmental Requirements

6.1 The Supplier shall comply in all material respects with all applicable environmental laws, permits and regulations in force in relation to the Contract.

6.2 The Supplier warrants that it has complied with the principles of ISO 14001 standards throughout the Term.

6.3 The Supplier shall meet the Government Buying Standards applicable to the Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs.

Part B – Sustainability and Reporting

1. Sustainability Requirements

1.1 The Supplier shall complete the Corporate Social Responsibility Report at Paragraph 3 of this Part B in relation to its provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.

1.2 The Supplier shall use reasonable endeavours to avoid the use of paper and card in carrying out its obligations under this Contract. Where unavoidable under reasonable endeavours, the Supplier shall ensure that any paper or card deployed in the performance of the Services consists of one hundred percent (100%) recycled content and used on both sides where feasible to do so.

1.3 The Supplier shall complete and provide CCS with a Carbon Reduction Plan.

1.4 The Supplier shall progress towards carbon net zero during the lifetime of the framework.

2. Social Value Requirements

2.1 The Supplier shall complete the Corporate Social Responsibility Report at Paragraph 3 of this Part B in relation its performance on meeting any Social Value obligations agreed to for the provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.

2.2 The Supplier shall use their best endeavours, as an organisation, to deliver environmental sustainability and protection in the provision of the Deliverables by establishing and delivering against credible targets for delivering energy efficiency throughout the lifetime of the framework.

2.3 The Supplier shall use their best endeavours, as an organisation, to address inequality in employment, skills and pay by supporting disadvantaged, underrepresented and minority groups into employment throughout the lifetime of the framework.

2.4 The Supplier shall use their best endeavours, as an organisation, to promote new opportunities and engage with new and small organisations (e.g. SMEs and VCSEs), to help them grow, supporting their development throughout the lifetime of the framework.

3. Reporting Requirements

3.1 The Supplier shall complete the Corporate Social Responsibility Report in relation to its provision of the Deliverables under this Contract and provide the Corporate Social Responsibility Report to the Buyer on the date and frequency outlined in Table A of this Part B.

3.2 The Supplier shall provide the baseline data contained within Table B (1) – Baseline data to facilitate subsequent measurement throughout the lifetime of the framework. The information required to populate Table B (1) and annually thereafter) will be provided to CCS within 10 calendar days of the submission of a request by CCS.

3.3 The Supplier shall complete the Framework Performance Indicator Submission Form at the frequency outlined in Table B of this Part B and return to CCS. The Supplier shall include in the Framework Performance Indicator Submission Form the content specified within Table B.

3.4 The Supplier shall attend Supplier Relationship Meetings with CCS at such times and frequencies as CCS determine from time to time to discuss the information contained in the Framework Performance Indicator Submission Forms. The information will be used to measure progress of social value activity.

3.5 In the event CCS develops an alternative social value measurement tool during the lifetime of the framework, the Performance Indicator measures described at Table B will be superseded by that tool.

Table A

Report Name	Content of Report	Frequency of Report
Sustainability	a. the key sustainability impacts identified; b. sustainability improvements made; c. actions underway or planned to reduce sustainability impacts; d. contributions made to the Buyer's sustainability policies and objectives; e. sustainability policies, standards, targets and practices that have been adopted to reduce the environmental impact of the Supplier's operations and evidence of these being actively pursued, indicating arrangements for engagement and achievements. This can also include where positive sustainability impacts have been delivered; and, f. risks to the Service and Subcontractors of climate change and severe weather events such as flooding and extreme temperatures including mitigation, adaptation and continuity plans employed by the Supplier in response to those risks.	Upon request by the Buyer and/or CCS.
Greenhouse Gas Emissions	Indicate greenhouse gas emissions making use of the use of the most recent conversion guidance set out in 'Greenhouse gas reporting – Conversion factors' available online at https://www.gov.uk/guidance/measuring-and-reporting-environmental-impacts-guidance-for-businesses.	Upon request by the Buyer and/or CCS.
Water Use	Volume in metres cubed.	Upon request by the Buyer and/or CCS.

Energy Use	Separate energy consumption figures for: a. assets deployed on the Supplier's site; b. assets deployed on the Authority's site; c. assets deployed off-site; and d. energy consumed by IT assets and by any cooling devices deployed. Power Usage Effectiveness (PUE) rating for each data centre/server room in accordance with ISO/IEC 31034-2/EN 50600-4-2.	Upon request by the Buyer and/or CCS.
Social Value	See the Supplier's response to question 6 of the Quality Questionnaire, within Call-Off Schedule 4 (Call-Off Tender).	As outlined within the 'Social Value Commitment' section of the Order Form, and other applicable Schedules throughout this Contract.

Table B – Submission to CCS

Report Name	Content of Report	Frequency of Report
Framework Performance Indicator Submission Form – Modern Slavery section	MSAT completion and progress recorded against the following 6 areas: ● Governance ● Policies and Procedures ● Risk Assessment and Management ● Due Diligence ● Training ● KPI	Annually.
Framework Performance Indicator Submission Form – Carbon Net Zero	The Supplier to demonstrate progression towards carbon net zero by reporting on the below areas: ● Number of carbon reduction activities that your organisation	Annually.

	has taken to progress your carbon reduction plan ● Number of RM6261 carbon reduction activities that benefit the Buyer ● List the top 3 carbon reduction activities completed for non RM6261 contracts	
Framework Performance Indicator Submission Form – Apprenticeships	Supplier shall submit data demonstrating how they are progressing apprenticeships within their organisation ● Number of apprenticeships started ● Cumulative number of apprenticeships ongoing ● Number of apprenticeships concluded ● Number of apprenticeships retained	Annually.
Framework Performance Indicator Submission Form – Diversity & Inclusion	To demonstrate that suppliers are redressing workforce imbalance within their organisation ● Representation of women ● Representation of ethnic minorities ● Representation of staff who identify as having a disability ● Representation of prison leavers ● Representation of LBTQIA+	Annually.
Framework Performance Indicator Submission Form – SMEs/VCSEs	To demonstrate that Suppliers are engaging with and developing SMEs/VCSES: ● Number of SMEs/VCSES within your supply chain for RM6261 ● Number of SME/VCSEs within your supply chain delivering services on RM6232 contracts ● How many sub-contract opportunities have there been within the reporting period ● Of the sub-contract opportunities, how many were awarded to a SMEs	Annually.

Table B (1) – Baseline data:

Report Name	Content of Report	Frequency of Report
Apprenticeships baseline data	The Supplier shall submit data demonstrating: • % of apprentices in their current workforce • % conversion rate of apprentices retained when an apprenticeship concludes	To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter.
Diversity of Workforce baseline data	The Supplier shall submit baseline figures of their current UK workforce: • Representation of women • Representation of ethnic minorities • Representation of staff who identify as having a disability • Representation of prison leavers • Representation of LBTQIA+	To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter.
SMEs/VCSEs baseline data	The Supplier shall produce and submit a SME / VCSE engagement strategy detailing how they intend to retain and develop SMEs/VCSEs within their supply chain.	To be provided to CCS within 10 calendar days of the submission of a request and annually thereafter.

Joint Schedule 6 (Key Subcontractors)

The Supplier may subcontract the Service to EE Limited ("**EE**") and will assign the benefit of Order to EE in respect of ordering, provision, maintenance, invoicing, and payment for the Service.

Key Sub- contractor name and address (if not the same as the registered office)	**Registered office and company number**	**Related product/Service description**	**Key role in delivery of the Services**
EE Limited	1 Braham Street, London, E1 8EE	Mobile Voice and Data provider, Service Provider	Primary Voice and Data Service provider

var

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)

Definitions

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

"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;

Status of the Controller

2. 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 2018. 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 the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 of this Joint Schedule 11 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 of this Joint Schedule 11 *(Processing Personal Data*) by the Controller.

4. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5. 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 Deliverables;

(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.

6. 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 of this Joint Schedule 11 *(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 of this Joint Schedule 11 *(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*) of the Core Terms;

(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 UK or 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 UK 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.

7. Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately 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.

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

9. 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 7 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.

10. 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 UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

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

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

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

13. 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.

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

15. The Relevant Authority may, at any time on not less than thirty (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).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. 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's Office.

Where the Parties are Joint Controllers of Personal Data

17. 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 UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

18. 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.

19. 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.

20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 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.

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

22. 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 UK GDPR); and

(c) where it has recorded it in Annex 1 of this Joint Schedule 11 *(Processing Personal Data).*

23. 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 UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25. 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.

26. 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.

27. 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 of this Joint Schedule 11 *(Processing Personal Data).*

28. 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 of this Joint Schedule 11 *(Processing Personal Data)*.

29. Notwithstanding the general application of paragraphs 2 to 16 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 paragraphs 18 to 28 of this Joint Schedule 11.

Annex 1 – Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: [redacted] Email – [redacted].

1.2 The contact details of the Supplier's Data Protection Officer are: Name: [redacted] Email address: [redacted] Address: 1 Braham Street, LONDON, E1 8EE

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Authorised Processing

Annex 1: a) Processing Personal Data – Contract Administration

- The contact details of the Relevant Authority's Data Protection Officer are recorded in the Call-Off Order Form.
- The contact details of the Supplier's Data Protection Officer are recorded in the Call-Off Order Form
- The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	The Parties are Independent Controllers of Personal Data The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: Business contact details of Supplier Personnel for which the Supplier is the Controller, Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,
Duration of the Processing	Up to six (6) Months after the expiry or termination of the Call Off Contract (including any Termination Assistance Period, where applicable).
Nature and purposes of the Processing	In respect of the Supplier Personal Data, CCS may collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Contract) to enable it to administer the Contract and fulfil tasks in the public interest and as required by law. This may include: • Inviting the Supplier Staff to contract management workshops and events;

	• Complying with requirements under the Contract to contract named individuals; • establishing the Supplier's compliance with the procurement process and the Contract; and • including Personal Data within reports. In respect of the Relevant Authority's Personal Data over which the Supplier shall act as a Controller, the Supplier may: collect, collate, share, evaluate, use, store, replicate, and otherwise Process the Personal Data (subject to the terms of the Contract) to enable it to administer and fulfil its obligations under the Contract. This may include: • administering, tracking and fulfilling Orders for the Services; • implementing all or any of the Services; • managing and protecting the security and resilience of any Supplier Equipment, the Supplier System and/or the Services; • managing, tracking and resolving Incidents associated with the Services as set out in the Call Off Contract; • administering access to online portals relating to the Services; and • compiling, dispatching and managing the payment of invoices. The Supplier and its suppliers, including any Sub-processors of the Supplier and its suppliers, may from time to time use back office support and system functions which are located or can be accessed by users from outside of the UK and/or the European Economic Area. The Buyer consents to the disclosure and transfer of Government Data, including Personal Data, as set out above in order to provide the Services. The Supplier will inform the Buyer of intended changes to its Sub-processors from time to time, either by providing the Buyer with online access to intended changes or by such other means as the Supplier may determine. If the Buyer does not object to the proposed change within 30 days' of this notice, the Buyer will be deemed to have authorised the use of the new Sub-processors. Due to the nature of the Services, Government Data will not be backed-up by the Supplier.
Type of Personal Data	Individuals' names, job titles, email addresses, organisational name, work phone numbers. To the extent relevant and supplied during the procurement process, details of any relevant convictions.
Categories of Data Subject	Relevant Authority Staff and Supplier Staff.
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	For the duration of the Contract and 7 years after.

Annex 1: b) Processing Personal Data – the Service

Description	Details
Identity of Controller for each Category of Personal Data	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor in accordance with Clause 14.1 of the Core Terms.
Duration of the Processing	For as long as the Supplier provides the Services and for as long as the Supplier may be required to Process the Personal Data in accordance with Law.
Nature and purposes of the Processing	The Services provide the Buyer with a mobile wireless communications service. The Supplier processes any information that is generated by the User's use of voice mail, voice recording, text messaging features and web browsing. Given that recordings can be made and stored, any type of Personal Data could be captured or provided inadvertently by the User. Any access to the content of such communications by the Supplier is strictly in accordance with Law. The Supplier and its suppliers, including any Sub-processors of the Supplier and its suppliers, may from time to time use back office support and system functions which are located or can be accessed by users from outside of the UK and/or the European Economic Area. Any such processing will be in accordance with Joint Schedule 11 Paragraph 6 (d) (i) to (iv). The Buyer consents to the disclosure and transfer of Government Data, including Personal Data, as set out above in order to provide the Services. The Supplier will inform the Buyer of intended changes to its Sub-processors from time to time, either by providing the Buyer with online access to intended changes or by such other means as the Supplier may determine. If the Buyer does not object to the proposed change within 30 days' of this notice, the Buyer will be deemed to have authorised the use of the new Sub-processors. Due to the nature of the Services, Government Data will not be backed-up by the Supplier.
Type of Personal Data	• name; • gender; • date of birth; • email address; • address; • telephone number; • associated persons; • contact notes from calls; • contact records; • family and friends' telephone numbers; • Personal Data traffic and communications records; and • recordings, including mobile voice and text message. This list is not exhaustive as the Buyer will specify what Buyer Personal Data is processed.

International transfers and legal gateways	• No data processing will take place outside of the UK.
Categories of Data Subject	• Users • Third party participants in voice calls or text messages to and from Users
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data for a different duration	All relevant data to be deleted six (6) Months after the expiry or termination of the Call-Off Contract (including any Termination Assistance Period, where applicable) unless longer retention is required by Law or the terms of the Call-Off Contract.

Annex 2 – Joint Controller Agreement

Not applicable – in accordance with this Joint Schedule 11 (Processing Data), for the purposes of the Data Protection Legislation, the Relevant Authority (the Buyer) is the Controller, and the Supplier is the Processor.

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 Joint 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 subject to Paragraph 2.3, advertise on Contracts Finder all Sub-Contract opportunities arising from or in connection with the provision of the Deliverables above a minimum threshold of £25,000 that arise during the Contract Period;

2.1.2 within 90 days of awarding a Sub-Contract to a Subcontractor, update the notice on Contracts 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 Joint 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 – Supply Chain Information Report template

Supply Chain Information Report templat

Call-Off Schedule 1 (Transparency Reports)

1. The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1). 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.

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.

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.

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

Title	Content	Format	Frequency
Service Transition Report	Overview of the number of End Users which have successfully: - Had eSIMs deployed - Had their number ported from the incumbent Supplier - Been fully transitioned to the Supplier's MVDS tariff.	To be agreed between the Parties. Expected to be Word, PDF, Excel, or any other applicable format.	Weekly from the Call-Off Start Date until the Supplier's MVDS solution has been implemented.
Call-Off Contract Charges	Overview of the invoices submitted with supporting management information (i.e., number of active connections within the preceding Month, Shared Data Bundle active within the preceding Month, etc).	To be agreed between the Parties. Expected to be Word, PDF, Excel, or any other applicable format.	Monthly.
Custom Reporting	The provision of custom reporting which allows the Buyer to analyse usage and connection data (at an organisational, grouped End User, and individual End User level) in detail.	To be agreed between the Parties. Expected to be Word, PDF, Excel, or any other applicable format.	Ad-hoc as required by the Buyer via the Supplier's online service portal (real-time) *and* a fully detailed report Monthly (provided by the Supplier).
Service Alerts	The Mobile Manager portal allows the DfE administrators to	Email.	When the Buyer is close to exceeding agreed data thresholds.

	set up alerts which will advise them of data thresholds met or exceeded during a billing cycle. These can be set at a data usage level, a percentage of consumption, or a selected spend. There can be multiple alerts set up at different parameters to suit DfE requirements.		
Performance Monitoring Report(s)	Report to show the Supplier's performance against the Service Levels identifed within Call-Off Schedule 14 (Service Levels).	To be agreed between the Parties. Expected to be Word, PDF, Excel, or any other applicable format.	Monthly.

Additional reporting requirements may be identified through the life of the Call-Off Contract – should this occur, the Parties shall agree on the content of such reporting requirements, alongside the format and frequency of which this will be delivered to the Buyer.

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 will 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 4 (Call Off Tender)

The Supplier's Tender Submission is outlined below:

Pass / Fail Questionnaire: [redacted]

Quality Questionnaire – Mobile V&DS 2025 – itt_3369: [redacted]

Pricing Schedule – Mobile V&DS 2025 – itt_3369:
[redacted]

Call-Off Schedule 5 (Pricing Details)

Total Call-Off Charges: **£173,124 exc. VAT.**

Charges Breakdown:

[redacted]

Payment Profile:

The Supplier will invoice the Buyer for Mobile Voice & Data services.

The Supplier will submit electronic invoices to the Buyer for Services monthly in arrears.

The Supplier will provide all invoicing and billing no later than four (4) months after the Services were delivered. The Buyer has the ability to approve or reject all invoices within 10 working days. All invoices presented to the Buyer for Services delivered more than four (4) months before provision of the invoice shall be invalid and the Buyer shall have no obligation or liability in respect of such invoices

The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.

The Supplier will provide supporting itemised management information in a format suitable to the Buyer at the end of each Service Management Period.

Invoices to be sent electronically to AccountsPayable.OCR@education.gov.uk in accordance with the billing process identified above. All invoices must include a valid Purchase Order number.

A copy of all invoices must also be sent to A copy of all invoices must also be sent to [redacted](Service Manager).

To request a statement, please email Accountspayable.BC@education.gov.uk.

The Buyer will pay the Supplier within 30 days of receipt of a valid invoice. An invoice will only be deemed valid if it is legible and includes:

- the date of the invoice;
- a unique invoice number;
- Supplier's full name and address;
- a valid DfE Purchase Order number (prefix – CORE-PO-);
- the charging period;
- a detailed line level breakdown of the appropriate Charges including Services provided;
- Charges in GBP (£); and,
- Payable UK VAT included as a separate line.

All invoices must also be in an un-editable format (such as PDF) and be in accordance with the Charges agreed with the Buyer, as outlined within this Call-Off Contract.

Invoices without a valid Purchase Order number are now rejected by the Buyer's e-invoicing solution. The Buyer no longer accepts paper invoices.

Call-Off Schedule 6 (ICT Services)

1. Definitions

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

"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
“Commercial off the shelf Software” or “COTS Software”	Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms
“Core Network”	the provision of any shared central core network capability forming part of the overall Services delivered to the Buyer, which is not specific or exclusive to a specific Call-Off Contract, and excludes any configuration information specifically associated with a specific Call_Off Contract;
"Defect"	any of the following: a) any error, damage or defect in the manufacturing of a Deliverable; or b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or

	the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;
"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
"Maintenance Schedule"	has the meaning given to it in paragraph 8 of this Schedule;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;

"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: a) the Deliverables are (or are to be) provided; or b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or c) where any part of the Supplier System is situated;
"Permitted Maintenance"	has the meaning given to it in paragraph 8.2 of this Schedule;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation

	instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

3. Buyer due diligence requirements

3.1. This paragraph 3 applies where the Buyer has conducted a Further Competition Procedure. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2. operating processes and procedures and the working methods of the Buyer;

3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2. The Supplier confirms that it has advised the Buyer in writing of:

3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

3.2.2. each aspect, if any, of the Operating Environment where the provision of the Services will be subject to site surveys, wayleaves and/or any other consents not yet granted;

3.2.3. the actions needed to remedy each such unsuitable aspect; and

3.2.4. a timetable for and the costs of those actions.

4. Licensed software warranty

4.1. The Supplier represents and warrants that:

4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Supplier shall:

5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3. ensure that the Supplier System will be free of all encumbrances;

5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

6.1. The Supplier shall, where requested by the Buyer as part of their Further Competition Procedure, develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**").

6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them.

Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:

6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

7.1. Subject to Paragraph 1.20 of Schedule 16 (Buyer Specific Security Requirements) as set out below, the Supplier shall allow any auditor access to the Supplier premises to:

7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

8.1. If requested by the Buyer as part of its Further Competition Procedure and specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (other than to the Core Network) (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance, including to the Core Network.

8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such

a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

of its own Existing IPR that is not COTS Software;

third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.2 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. **Licenses for COTS Software by the Supplier and third parties to the Buyer**

9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

9.4. **Buyer's right to assign/novate licences**

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. **Licence granted by the Buyer**

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. **Open Source Publication**

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to

be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. **Malicious Software**

9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third-party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. Supplier-Furnished Terms

10.1. **Software Licence Terms**

Not applicable.

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Order Form 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.

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"	a plan which details the processes and arrangements that the Supplier shall follow to: (a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and (b) the recovery of the Deliverables in the event of a Disaster;
"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);
“Standard BCDR Plan”	means the Supplier’s standard BCDR Plan;
“Supplier Group”	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of Part B of this Schedule;

Part A: BCDR Plan – Short Form

Unless otherwise specified in this Schedule, this Part A shall apply only to Call-Off Contracts which have been awarded via Direct Award in accordance with Framework Schedule 7 (Call-Off Contract Award Procedure).

1. BCDR PLAN

1.1 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.

1.2 Promptly (and in any event within 30 days) after the Start Date, the Supplier shall provide to the Buyer its Standard BCDR Plan.

1.3 The Supplier shall ensure at all times that its Standard BCDR Plan conforms with Good Industry Practice.

1.4 The Supplier may from time to time during the Contract Period review, update, and/or test its Standard BCDR Plan. The Supplier shall ensure that any use by it or any Subcontractor of "live" Buyer 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.

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

1.5.1 the outcome of the test;

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

1.5.3 the Supplier's Proposals for remedying any such failures.

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

1.7 To the extent the Standard BCDR Plan contains processes, procedures, and/or other content which is designed to permit the continuity of the business operations of the Buyer supported by the Deliverables through continued provision of the Deliverables following an Insolvency Event of the Supplier, any Key Sub-contractor and/or any Supplier, the Standard BCDR Plan shall be invoked by the Supplier:

where an Insolvency Event of a Key Sub-contractor and/or Supplier Group member (other than the Supplier) could reasonably be expected to adversely affect delivery of the Deliverables; and/or

where there is an Insolvency Event of the Supplier, and the insolvency arrangements enable the Supplier to invoke the plan.

Part B: BCDR Plan – Long Form

This Part B shall apply to all Call-Off Contracts which have been awarded via a Further Competition procedure in accordance with Framework Schedule 7 (Call-Off Contract Award Procedure) and shall not apply to any Call-Off Contracts awarded via Direct Award.

1. BCDR Plan

The Parties shall comply with the terms set out in Part A of this Schedule.

Call-Off Schedule 9 (Security)
Part A: Short Form Security Requirements

1 Definitions

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

"Breach of Security"	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, 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"	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 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.

Call-Off Schedule 11 (Installation Works)

1 When this Schedule should be used

1.1 This Schedule is designed to provide additional provisions necessary to facilitate the provision of Deliverables requiring installation by the Supplier.

2 How things must be installed

2.1 Where the Supplier reasonably believes it has completed the Installation Works, it shall notify the Buyer in writing. Following receipt of such notice, the Buyer shall inspect the Installation Works and shall, by giving written notice to the Supplier:

2.1.1 accept the Installation Works, or

2.1.2 reject the Installation Works and provide reasons to the Supplier if, in the Buyer's reasonable opinion, the Installation Works do not meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract).

2.2 If the Buyer rejects the Installation Works in accordance with Paragraph 2.1.2, the Supplier shall immediately rectify or remedy any defects and if, in the Buyer's reasonable opinion, the Installation Works do not, within five (5) Working Days of such rectification or remedy, meet the requirements set out in the Call-Off Order Form (or elsewhere in this Contract), the Buyer may terminate this Contract for material Default.

2.3 The Installation Works shall be deemed to be completed when the Supplier receives a notice issued by the Buyer in accordance with Paragraph 2.1.1. Notwithstanding the acceptance of any Installation Works in accordance with Paragraph 2.1.1., the Supplier shall remain solely responsible for ensuring that the Goods and the Installation Works conform to the specification in the Call-Off Order Form (or elsewhere in this Contract). No rights of estoppel or waiver shall arise as a result of the acceptance by the Buyer of the Installation Works.

2.4 Throughout the Contract Period, the Supplier shall have at all times all licences, approvals and consents necessary to enable the Supplier and the Supplier Staff to carry out the Installation Works.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

1 Definitions

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 Part A of this Schedule shall only apply if the Contract was entered into as a result of the Buyer undertaking a Further Competition in accordance with Framework Schedule 7.

2.2 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan within five (5) Working Days after the Call-Off Contract Start Date.

2.3 The draft Implementation Plan:

2.3.1 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and

2.3.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

2.4 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.

2.5 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.

2.6 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 3.3, 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 Failure by the Supplier to Achieve a Milestone by the relevant Milestone Date, where such failure is caused by or is attributable to the acts and/or omissions of the Supplier shall constitute a material Default and shall entitle the Buyer to terminate the Contract.

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 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.

4.5 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 entitled to or does terminate this Contract pursuant to Clause 10.4 of the Core Terms (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 of the Core Terms (How much you can be held responsible for).

7 Implementation Plan

7.1 The Implementation Period will be a two (2) 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 an 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 an 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

The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

[redacted]

Part B – Testing

In accordance with Special Term 2, 'Part B – Testing' of Call-Off Schedule 13 (Implementation Plan and Testing) will be deleted in its entirety, and shall not apply to this Contract. The Services shall be deemed as successfully implemented once:

- eSIMs have been deployed to all applicable End Users;
- phone numbers have been ported from the incumbent supplier for all End Users; and,
- all End Users have been transitioned to the Supplier's Mobile Voice and Data Solution.

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):

“Critical Service Level Failure”	has the meaning given to it in the Order Form;
"Service Credits"	any service credits (in respect of Lot 2, Lot 3 and Lot 4 Deliverables only) specified in the Annexes to Part A of this Schedule and/or any Order Form being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Order Form;
"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 Annexes to Part A of this Schedule and in any Order Form; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annexes to Part A of this Schedule or the Order Form (as applicable).

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 CCS and the Buyer to the rights set out in Part A of this Schedule. The Supplier further acknowledges that those rights in respect of any Service Level Failure will include, where agreed in an Order Form in respect of Lot 2, Lot 3 and/or Lot 4 Deliverables, 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: (i) CCS in respect of the Service Levels for Lot 1; and (ii) the Buyer in respect of the Lot 2, 3 & 4 Service Levels in accordance with the provisions of Part B (Performance Monitoring) of this Schedule, detailing the level of service which was achieved.

2.4 Where Service Credits have been agreed, 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 entitled to or does terminate this Contract pursuant to Clause 10.4 of the Core Terms (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, CCS or 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 or Buyers' 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: (i) the CCS Authorised Representative in writing in relation to any failure in respect of Lot 1 Service Levels; or (ii) the Buyer in writing in relation to any failure in respect of Lot 2, 3 or 4 Service Levels. CCS or the Buyer (as applicable), 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 of the failure 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 (applicable to Lot 2, Lot 3 and Lot 4 only)

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 the calculation formula in the Annexes to Part A of this Schedule and as otherwise agreed in the Order Form.

Annex A to Part A: Service Levels for Lot 1

The following are included as the Service Levels that the Supplier must meet for each Buyer procuring Lot 1 Deliverables under this Framework Contract.

Service Levels					
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Failure	Service Level Threshold	Measurement (Business Hours/ Operational)
Availability of Coverage	Coverage		99%	99.5%	Operational Hours
LTE Accessibility LTE Retainability Call Set Up Success Rate LTE data download LTE data upload	Performance		99% 99% 99% 5 1	99.5% 99.5% 99.5% 10 4	Operational Hours
Availability of Self Service Portal	Availability	For Self Service Portal the Supplier shall be allowed to request a maximum of 8 hrs Service Downtime for Permitted Maintenance in any one Service Period which shall take place between 20:00 and 06:00 hr			Operational Hours
Call answered within 20 seconds Calls abandoned Acknowledgement of email enquiries, including billing Resolution of email enquiries, including billing	Customer Services	At all times Within 24 hours Within 24 hours of receipt Within 5 working days of receipt	75% >10 85% 90%	80% >5 90% 95%	Business Hours

Incident Management Fix Times Priority One Priority Two Priority Three Priority Four Incident Management Response Times Priority One Priority Two Priority Three Priority Four	Service Management	 4 hours 8 hours 3 working days 5 working days 15 mins 30 mins 1 hour 8 hours	 90% 85% 85% 85% 90% 85% 80% 75%	 95% 90% 90% 90% 95% 90% 85% 80%	 Operational Hours Business Hours

Definitions:

Coverage: Availability is Cell Site Availability offering access to the Mobile Communications (total no. of hours not operational / total no. of hours x 100%)

Agreement at call off level can include reduced areas of interest e.g. region rather than national and/or inclusion of specific areas of interest

LTE Accessibility: Availability to access the LTE network/bearer

LTE Retainability: Availability of remaining to be connected to the LTE network/bearer

Call Setup Success Rate: Ability to set up a call with a normal closure code

LTE Data Download: Average Download

Incident Management Fix Times, Priority One: Total loss of service impacting a customer (greater than 80% of Users from accessing the Service) where a wider network issue is impacting the majority (>80%) of the suppliers customers

Incident Management Fix Times, Priority Two: Total loss or partial loss of service impacting a customer (greater than 50% of Users from accessing the Service) where a wider network issue is impacting many (>50%) of the suppliers customers, and or loss of coverage at a key strategic location (as agreed between the parties)

Incident Management Fix Times, Priority Three: Loss or partial loss of service which has a substantial impact on a customer ability to carry out its duties, and impacting more than 10% of Users

Incident Management Fix Times, Priority Four: Partial loss or restriction of services which has moderate impact on the Customer to carry out its duties, and impacting less than 10% of Users

Annex B to Part A: Service Levels for Lot 2

The Buyer may specify Service Levels in respect of Lot 2 Deliverables in the Order Form.

Where: (i) a Buyer does not specify Service Levels in an Order Form in respect of Lot 2 Deliverables; and (ii) the Lot 2 Deliverables are the same or substantially similar to the Lot 1 Deliverables, those Service Levels set out in Annex A to Part A of this Schedule will apply to those Lot 2 Deliverables.

Service Levels				**Service Credit for each Service Period**	**Publishable KPI**
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**		
Implementation Timescales	Deployment of all eSIMs, porting of numbers from incumbent Supplier, and transition to Supplier's MVDS tariff.	No later than 31st May 2025	No later than 31st May 2025	2.5% Service Credit (payable against first Month's billing if any implementation activities exceed 31st May 2025)	Not applicable.
Availability of Service Coverage - Network	Coverage	at least 99% at all times	At least 99.5% at all times	Not applicable	As required by the Buyer
Availability of Online Portal – Self Service Management	Availability	at least 99.9% at all times (excluding planned downtime)	at least 99.9% at all times (excluding planned downtime)	Not applicable	As required by the Buyer
Service Response Times	Service Management	P1 (Critical): 4 hours	P1 (Critical): 15 MINS P2 (High): 30 MINS	0.25% Service Credit gained for each	As required by the Buyer

Service Levels				Service Credit for each Service Period	Publishable KPI
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**		
		P2 (High): 8 hours P3 (Medium): 48 hours	P3 (Medium): 1 HOUR P4 (Low): 8 HOURS	percentage under the specified Service Level Performance Measure	
Incident Management Fix Times	Service Management	P1 (Critical): 4 hours P2 (High): 8 hours P3 (Medium): 48 hours P4 (Low): 5 working days	P1 (Critical): 4 hours P2 (High): 8 hours P3 (Medium): 48 hours P4 (Low): 5 working days	0.25% Service Credit gained for each percentage under the specified Service Level Performance Measure	As required by the Buyer
Social Value KPI	Service Management	Number of young people reached through each event – Target 100 Number of events each year of contract – Target 2/3 FY1, growing to 4/5 FY3	Number of young people reached through each event – Target 100 Number of events each year of contract – Target 2/3 FY1, growing to 4/5 FY3 % of young people saying this helped them with understanding online risks – Target +75% Store follow up visits by family – Target of 10+ Summary report to be sent	Not applicable.	Number of volunteering hours delivered annually.

Service Levels				Service Credit for each Service Period	Publishable KPI
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**		
		% of young people saying this helped them with understanding online risks – Target +75% Store follow up visits by family – Target of 10+ Summary report to be sent Number of volunteering hours committed – 5+ hours	Number of volunteering hours committed – 5+ hours		

The Service Credits shall be calculated on the basis of the following formula:

Formula: (x% (Service Level Performance Measure) - x% (actual Service Level performance))*0.25	=	x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Worked example: (98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period))*0.25	=	5.75% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Part B: Performance Monitoring

1. Performance Monitoring and Performance Review

1.1 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.

1.2 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:

1.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

1.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

1.2.3 details of any Critical Service Level Failures;

1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

1.2.5 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

1.2.6 such other details as the Buyer may reasonably require from time to time.

1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") as required by the Buyer (see the Annex: Contract Boards of Call-Off Schedule 15 (Call-Off Contract Management). 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:

1.3.1 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;

1.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

1.3.3 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.

1.4 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.

1.5 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.

2. Satisfaction Surveys

2.1 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;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project 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 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 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 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:

- Following Contract execution, the Supplier will be required to attend an **initiation meeting** with the Buyer to agree the delivery methodology to provide the Services.
- **Service / Performance Review Meetings** – throughout the term of the Call-Off Contract, the Supplier will be required to attend regular meetings (frequency to be agreed between the Parties following the commencement of the Contract), to discuss the Supplier's overall performance which shall include at a minimum (but may not be limited to):
    - adherence to contractual obligations;
    - performance against Service Levels (as outlined within Call-Off Schedule 14 (Service Levels);
    - any Service issues; and,
    - review of the Contract risk register.

Call-Off Schedule 16 (Benchmarking)

1. DEFINITIONS

In this Schedule, the following expressions shall have the following meanings:

"Benchmark Review"	a review of the Deliverables carried out in accordance with this Schedule to determine whether those Deliverables represent Good Value;
"Benchmarked Deliverables"	any Deliverables included within the scope of a Benchmark Review pursuant to this Schedule;
"Comparable Rates"	the Charges for Comparable Deliverables;
"Comparable Deliverables"	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"	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"	data derived from an analysis of the Comparable Rates and/or the Comparable Deliverables (as applicable) provided by the Comparison Group;
"Good Value"	that the Benchmarked Rates are within the Upper Quartile; and
"Upper Quartile"	in respect of Benchmarked Rates, 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 will 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 of the Core Terms (Changing the contract).

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

This Schedule should be read and interpreted in conjunction with Call-Off Schedule 4 (Call-Off Tender).

1. INTRODUCTION

1.1. The Department for Education (DfE) is the department for realising potential. We enable children and learners to thrive, by protecting the vulnerable and ensuring the delivery of excellent standards of education, training, and care. This helps realise everyone's potential – and that powers our economy, strengthens society, and increases fairness.

1.2. The DfE's Technology Directorate's aim is to deliver high quality IT services to enable its end users (internal DfE staff) to support in delivering departmental objectives and priority outcomes. The End User Compute (EUC) team is responsible for providing IT hardware, productivity and collaboration tools to DfE's staff of approximately 8000 users.

1.3. The provision of Mobile Phone Handsets and a Mobile Voice & Data Service (***"MVDS"***) falls under the remit of the EUC team, and is an enabler, providing DfE staff *(**"End Users"***) with effective tooling to perform their job and maximise productivity.

2. CURRENT SITUATION AND FUTURE AIMS

2.1. DfE utilises Microsoft 365 as its core productivity suite, aswell as Microsoft Intune as its mobile device management (***"MDM"***) solution (including for mobile phones).

2.2. End Users are currently offered three different options for a telephony service:

2.2.1. Softphone capability on a DfE provided laptop (via MS Teams);

2.2.2. A Bring-Your-Own-Phone (BYOP) services, where End Users can access DfE data and systems via their personal mobile device; and,

2.2.3. A corporate mobile phone handset provided by DfE.

2.3. This ITT relates specifically to End Users who utilise a corporate mobile phone handset as their telephony service, as an associated Mobile Voice & Data Service is required.

2.4. Currently, there are approximately 4100 End Users with a corporate mobile phone handset. This number fluctuates based on the number of starters and leavers into the department, and whether those starters and leavers opted for a corporate mobile phone as their chosen telephony service.

2.5. All End Users who choose a corporate mobile phone handset as their telephony service are provisioned with an Apple iPhone SE (3rd gen). These devices are 'fully managed' using a COBO (corporate owned, business only) device management model. Apple Business Manager is used alongside Microsoft Intune for initial device enrolment and ongoing management.

2.6. DfE also utilises ServiceNow for asset management, and has an active sync between ServiceNow and Active Directory with the aim of End User details within the asset register being accurate and up to date. Additionally, there is an active sync between Microsoft Intune and Active Directory.

2.7. DfE's existing contract for the provision of MVDS ends on 31st May 2025.

2.8. Under this existing MVDS, DfE currently has access to:

2.8.1. An all-inclusive voice and SMS tariff;

2.8.2. A flexible shared data bundle pooled across all End Users, with the ability to increase or decrease the total data allowance based upon DfE current usage; and,

2.8.3. A small volume of unlimited data SIMs (managed separately from the shared data bundle) for certain VIPs and high-volume data users.

Physical nano SIMs are utilised for all connections.

2.9. As the existing MVDS contract is ending, DfE now have a requirement to procure a replacement Contract for the provision of Mobile Voice and Data Services to provide service continuity for End Users.

2.10. Mobile Phone Handsets are procured independently of DfE's MVDS contract, and as such, the provision of such devices is out of scope of this ITT.

3. SPECIFICATION

MOBILE VOICE AND DATA SERVICES

3.1. DfE is seeking the provision of a Mobile Voice and Data Service Contract which provides access to services on a like-for-like basis (i.e., an all-inclusive voice & SMS tariff for 4100 End Users, a flexible pooled shared data bundle, and access to unlimited data SIMs).

3.2. DfE **must** have the ability to add or remove connections (in respect to all MVDS products), with no minimum or maximum constraints on volumes. There **must** be no early termination fee payable should DfE choose to reduce the total number of connections.

3.3. DfE expects that the all-inclusive voice & SMS tariff will include the following call types, and shall further meet the minimum requirements of the RM6261 Framework Specification (but may not be limited to):

3.3.1. UK Landlines (i.e., starting with 01, 02, 03);

3.3.2. UK Mobiles (i.e., starting with 07);

3.3.3. UK non-geographic numbers (i.e., starting with 0300, 0800, 0808, and 116);

3.3.4. SMS; and,

3.3.5. Voicemail functionalities and retrieval.

Potential Providers **must** not apply a cap / usage limit to the Services provided under the all-inclusive voice & SMS tariff. Any excessive usage will need to be notified to the Buyer through reporting. Potential Provider's should provide details on any 'fair-usage policy' in place within their Call-Off Tender.

3.4. Outside of the all-inclusive voice & SMS tariff, End Users may have a business requirement to make calls / SMS to International and/or Premium Rate numbers. These calls / SMS should be charged by the Potential Provider on a pay as you consume (PAYC) basis. Potential Providers should provide a separate rate card as an attachment for any PAYC charges which may be applicable during the Call-Off Contract.

3.5. DfE should have the ability to restrict End Users from making any calls / SMS which fall outside of the scope of the all-inclusive voice & SMS tariff. DfE's EUC team should be able to manage the application of any restrictions on an individual and/or grouped End User basis.

3.6. Potential Provider's **must** always allow calls to emergency numbers regardless of any restriction in place.

3.7. The MVDS solution provided by the Potential Provider **must** also support 5G as a default, and allow for Wi-Fi Calling.

3.8. Having recently completed the refresh of its corporate mobile phone handsets to fully managed Apple iPhone SE's (3rd gen), DfE would also like to transition to the provision of MVDS via eSIMs as standard, rather than End Users utilising physical nano SIMs. Physical nano SIMs **must** remain available for specific use cases, e.g. where a minister utilises a

tablet that requires a 5G connection but is not eSIM compatible.

3.9. DfE would also like to improve the management of its End User data, so that asset / user records within its MVDS estate are more accurate, and are kept up to date on an ongoing basis to reflect any (and all) changes made.

3.10. The Contract is expected to commence on 1st April 2025 and will run for an initial term of 3-years and 2-months, until 31st May 2028. There shall be an optional extension provision included which allows for the Contract to be extended by up to a further 1-year, with a maximum Contract End Date of 31st May 2029.

DEPLOYMENT OF ESIMS AND TRANSITION TO NEW TARIFF

3.11. Potential Providers should note that the intention to commence the Contract on 1st April 2025 is to provide sufficient time for the successful Supplier to transition End Users onto eSIMs and the new tariff prior to the expiry of the current MVDS contract. The successful Supplier **must** ensure that all End Users have been transitioned to the replacement MVDS service prior to 31st May 2025.

3.12. DfE have no preference for how Potential Providers plan to transition End Users to the new MVDS tariff (i.e., bulk transition of all End Users or phased transition in batches). Potential Providers **must** provide details of their intended transition approach within their Call-Off Tender.

3.13. As part of the transition, all End Users **must** be provided with an eSIM to connect to the new tariff.

3.14. DfE expects that input from its End Users to install their eSIM should be minimal, and would prefer for Potential Providers to offer 'zero touch provisioning'.

3.15. With this in mind, delivery via 'eSIM push' is preferable, where the EUC team/successful Supplier pushes out the eSIM from an MDM, and the End User only needs to click on a push notification. Delivery via 'eSIM pull', where the End User must take action to initiate the installation of their eSIM (e.g. by scanning a QR code) is acceptable where eSIM push cannot be provided by the Potential Provider. All Potential Provider's **must** provide details of their intended delivery approach for the installation of eSIMs within their Call-Off Tender.

3.16. DfE requires Potential Providers to provide easy to follow communications and guidance documents so that End Users can navigate the end-to-end process for implementing an eSIM, without extensive support being required from internal DfE IT support teams.

3.17. The successful Supplier **must** work with DfE and the incumbent Supplier (if necessary) to port each number from the current network provider to the replacement network provider, ensuring all DfE End Users retain their existing phone number.

3.18. Potential Provider's **must** provide a draft high-level implementation plan within their Call-Off Tender response which outlines their intended approach, and estimated timescales for; the deployment of eSIMs, transition to new MVDS tariff, porting of numbers (e.g., bulk or in tranches), and planned commencement date of the replacement MVDS solution.

FLEXIBLE DATA BUNDLE

3.19. DfE requires a Shared, 5G Data Bundle for UK roaming that can be flexed up and down without penalty.

3.20. For the purposes of the evaluation process and calculating Contract Charges, Potential Providers should assume that DfE requires a 5TB Shared Data Bundle on a monthly basis. However, Potential Providers must also provide a rate card within their Pricing Questionnaire response which details the Unit Cost of Shared Data Bundles in pre-defined 'tiers'. This rate card **must** also include a separate line which clearly defines the cost for 'Out of Bundle Charges (OOB)', with the Potential Provider detailing how this would be chargeable (i.e., per GB and/or per MB).

3.21. The rate card should detail the different 'tiers' of Shared Data Bundles which Potential Providers can supply, with volume increments being as small as is reasonably possible (i.e., ideally DfE would like increments to be in 100-250GB increments), so DfE are able to flex volumes based on demand without having to under and/or over commit.

3.22. The monthly Charge for the applicable Shared Data Bundle **must** remain fixed, irrespective of the number of connections that will be consuming data under the Bundle.

3.23. DfE **must** have the ability to add or remove connections utilising data under the Shared Bundle, with no minimum or maximum constraints on volumes. There **must** be no early termination fee payable should DfE choose to reduce the total number of connections.

3.24. DfE expects the successful Supplier to work in collaboration with us to ensure that no overage Charges are incurred. Potential Providers should outline within their Call-Off Tender, the methodology which would be applied to ensure data usage is effectively tracked/managed (e.g., alerts if DfE are close to Shared Data Bundle limit, reporting to show End Users with high data consumption, recommendations to move specific End Users to unlimited data SIMs, review of business compliant usage for End Users with high data consumption, etc).

3.25. DfE **must** have the ability to assign data usage caps on an individual and/or grouped End User basis.

3.26. Potential Providers should outline within their Call-Off Tender what data utilisation is covered by the Shared Data Bundle, and what data utilisation would fall out of scope and be an additional PAYC Charge (e.g., countries covered by the Shared Data Bundle, EU / International Roaming charges, etc). Potential Providers should provide a separate rate card as an attachment for any PAYC Charges which may be applicable during the Call-Off Contract.

3.27. Outside of the Monthly Shared Data Bundle, DfE requires a small volume of unlimited data SIMs, which will be managed independently.

3.28. There **must** be no minimum term applicable for the unlimited data SIMs, and DfE **must** have the ability to activate, disconnect, and re-activate unlimited data SIMs without penalty.

3.29. Unlimited data SIMs **must** be available, for specific use cases, as physical nano SIM cards aswell as eSIMs.

SELF SERVICE MANAGEMENT PORTAL

3.30. Potential Provider's **must** provide DfE with access to an online portal to manage the MVDS solution, which **must** include the ability for DfE's IT support teams to make 'self-service' amendments.

3.31. This online portal **must** be available 99.8% at all times, which shall exclude any planned downtime. Any planned downtime **must** be communicated to DfE in advance, and should take place outside of UK business hours, and preferably overnight (between 20:00 and 06:00).

3.32. The EUC team within DfE has a dedicated IT support team who are responsible for managing the MVDS. To improve service efficiency, DfE would like to amend all elements of the MVDS themselves via 'self-service' functionality, with any applicable service amendments applied immediately.

3.33. If 'self-service' is available as a functionality but service amendments cannot be applied immediately, Potential Providers **must** outline within their Call-Off Tender response any timescale restrictions that apply (per each relevant service amendment).

3.34. Potential Providers **must** also outline within their Call-Off Tender response the level of 'self-service' functionality that can be provided through their online portal.

3.35. If there are any actions that DfE will not be able to complete as 'self-service', Potential Providers **must** also clearly outline within their Call-Off Tender which service amendments cannot be actioned via 'self-service' alongside the process for such service amendments being made and associated timescales for completion (i.e., ticket raised to Supplier Account team).

3.36. The Potential Provider's online portal **must** allow for multiple 'user role levels' to be applied, with different permission levels. The self-service portal **must** have multiple roles with different permission levels available (such as; administrator users, support team 2nd line permissions, read-only, etc).

3.37. The DfE EUC team (administrator users) should be able to set up and/or remove user accounts for DfE staff (as required), including the ability to set permission levels.

3.38. DfE **must** be able to access comprehensive usage and billing reporting via the successful Supplier's online portal, which shows real time service data (where possible). DfE **must** be able to run 'custom reporting' via the online portal at any time to support internal service management.

3.39. If Potential Providers are unable to show real time service data within their online portal, they **must** outline within their Call-Off Tender response the timescale delay which would be applicable.

3.40. Potential Provider's should outline within their Call-Off Tender response what 'custom reporting' can be run by DfE within the online portal. DfE's aim is for reporting to allow for the analysis of usage and connection data (at an organisational, grouped End User, and individual End User level). At a minimum, DfE expects reporting to be available which shows when an End User/eSIM/SIM was last connected to the network, so that this can be corroborated against 'zero usage' to optimise MVDS spend.

3.41. Although DfE are core users of the MVDS, a small volume of End Users are staff from two (2) of DfE's Arm's Length Bodies – Office of the Children's Commission (OCC) and Social Work England (SWE). Potential Provider's **must** be able to split DfE, OCC, and SWE into separate entities (with End Users grouped) which are managed under the same account. OCC End Users are managed by DfE directly; however, Potential Provider's **must** be able to provide standalone access to the online portal for SWE to manage their own estate. SWE **must not** be able to view DfE or OCC End User data.

3.42. Potential Provider's **must** also provide separate billing for DfE, OCC, and SWE, with each invoice only including Services which have been consumed by the applicable entity.

3.43. As part of service implementation/transition, the successful Supplier **must** provide training to applicable DfE users on how to effectively operate the online portal (with specific regard to 'self-service' functionalities). DfE's preference is for this to be conducted via online videoconferencing meeting(s). Such training **must** be provided prior to 31st May 2025 and/or the replacement MVDS going live (whichever is the earliest).

3.44. Potential Providers should detail their intended approach to training within their Call-Off Tender. At a minimum, DfE require separate training sessions to be provided for; the EUC team which covers the wider portal functionality, and internal IT support teams which covers basic support actions.

3.45. In addition to initial training, the successful Supplier should also provide additional access to training materials and/or guidance which DfE support team users are able to access on an ongoing basis, detailing how to effectively operate the online portal and 'self-service' functionalities.

MANAGEMENT OF USER DATA

3.46. DfE are keen to improve the ongoing management and maintenance of End User data, so MVDS service records are as accurate as possible.

3.47. To support this, DfE would like the ability to integrate/sync the successful Supplier's online service management portal with existing DfE tooling to streamline and automate certain processes. Ideally this would be via Microsoft Entra or Active Directory, but Potential Providers should outline if integration/syncs with ServiceNow may also be an option.

3.48. When a new End User is added to the MVDS, DfE's aim is for their user data to be searched/extracted from an existing database, rather than relying on manual input of data (reducing the potential human error). At a minimum, DfE expect the user data being pulled to include names and email addresses.

3.49. Where integrations are not available and manual input is required in the successful Supplier's online portal, certain fields with key data should be made mandatory so they cannot be left blank, to improve on the consistency of data.

3.50. DfE would like for the successful Supplier to allow custom attributes to be added to an End User's record within the MVDS to help further improve management (e.g. adding unique employee ID, VIP status, reasonable adjustments or disabilities, etc.).

3.51. In the event an End User changes their name (and subsequently their DfE email address is updated), DfE would like for their user data records within the successful Supplier's system to automatically be updated via integrations.

3.52. DfE would also like to understand what two-way integration/sync options Potential Providers can offer. An example of ideal functionality would be for an End User's mobile phone number to automatically be pulled into their M365 account.

3.53. Potential Provider's **must** outline within their Call-Off Tender response what integrations/syncing with existing DfE tooling they can support to help DfE improve the ongoing management and maintenance of End User data.

3.54. Potential Provider's should also describe how they can support DfE during service transition to ensure that data records across the Supplier's and DfE's systems are as closely linked as possible.

SERVICE COVERAGE

3.55. End Users who are utilising the MVDS solution may be based within any of DfE's office locations, which are outlined below (but may be subject to change during the life of the Contract):

Office Location	**Address**
Bristol	Second Floor, 3 Glass Wharf, Avon Street, Bristol, BS2 0EL
Cambridge	Eastbrook, Shaftesbury Road, Cambridge, CB2 8DR
Coventry	Cheylesmore House, 5 Quinton Road, Coventry, CV1 2WT
Croydon	Fifth Floor, Trafalgar House, 1 Bedford Park, Croydon, CR0 2AQ
Darlington	Bishopsgate House, Feethams, Darlington, DL1 5QE
Exeter	The Senate, Southernhay, Exeter, EX1 1UG

Leeds	7 & 8 Wellington Place, Wellington Street, Leeds, LS1 4AP
London	Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
Manchester	Piccadilly Gate, Store Street, Manchester, M1 2WD
Newcastle	Ground Floor, Newcastle Civic Centre, Barras Bridge, Newcastle upon Tyne, NE1 8QH
Nottingham	Fifth Floor, 1 Unity Square, Queensbridge Road, Nottingham, NG2 1AW
Sheffield	2 St Paul's Place, 125 Norfolk Street, Sheffield, S1 2FJ
Watford	Third Floor, 34 Clarendon Road, Watford, WD17 1JJ

3.56. Standard MVDS usage (within business hours) is likely to be in and around the vicinity of DfE's office locations. However, certain End Users may have home working contracts, and may live in remote locations.

3.57. Therefore, Potential Provider's **must** be able to provide high quality service Coverage across the UK (England, Scotland, Wales and Northern Ireland). Availability of Coverage **must** be available 99.0% at all times.

3.58. If during the term of the Contract, it is deemed that service Coverage is inadequate for any End User, the successful Supplier will be expected to work in collaboration with DfE to identify resolutions, which may include Coverage enhancement solutions, and/or providing access to another network provider's MVDS services. Any such Services shall not be Chargeable.

4. QUALITY AND CONTRACT / SERVICE MANAGEMENT

4.1. The successful Supplier **must** provide a single-point-of-contact for DfE throughout the life of the Contract, aswell as appropriate escalation contacts (tiered upwards). Where Potential Provider's may choose to provide DfE with a dedicated Account Management team, this should be clearly outlined (with assigned user roles) within their Call-Off Tender.

4.2. The supplier should look for methods to continually improve the service throughout the duration of the Contract (in accordance with Call-Off Schedule 3 (Continuous Improvement)).

4.3. Potential Provider's **must** provide DfE with access to an online service desk portal to raise any support requests. At a minimum, this service desk should be accessible between 08:00 – 17:00 Monday to Friday (excluding bank holidays). This online service desk portal may be the same system as the online portal which is provided by the Potential Provider for DfE to manage the MVDS solution. The online service desk **must** be available 99.8% at all times, which shall exclude any planned downtime.

4.4. Any support request which is raised by DfE **must** be assigned a 'priority category' depending on the criticality of the response raised. Potential Provider's **must** outline within their Call-Off Tender initial acknowledgement / response times to support requests raised,

and subsequent fix times for such support requests. Potential Provider's should also aim to identify any service levels which may be applicable to queries raised outside of the online service desk portal (i.e., phone calls, email queries, billing queries, etc).

4.5. Throughout the Contract, the Supplier will be required to provide relevant reporting and attend progress meetings with/to DfE on a regular basis. The frequency and most appropriate mechanism for such reports and meetings will be agreed between the Parties following Contract Award (based upon the responses provided by the Supplier to the 'Quality Questionnaire – Mobile V&DS 2025 – itt_3369').

4.6. Potential Providers should refer to Call-Off Schedule 14 (Service Levels) which is applied to this Further Competition, and which will require finalisation prior to Contract execution. The Supplier will be expected to work with DfE to agree the parameters for Service Levels/KPIs which will be applied to Contract following Contract Award (based upon the responses provided by the Supplier to the 'Quality Questionnaire – Mobile V&DS 2025 – itt_3369'). Examples of Service Levels which may be applied include but are not limited to; implementation timescales, availability of Service Coverage, availability of Supplier Online Portal(s), service response times, Social Value KPI, etc.

5. EXIT MANAGEMENT

5.1. For the avoidance of doubt, Call-Off Schedule 10 (Exit Management) **will not** be applied to this Contract. The successful Supplier will be required upon Contract Exit to provide service transition support as is regulated by Ofcom.

6. SECURITY CONSIDERATIONS

6.1. Potential Providers **must** ensure that they (and any Subcontractors and/or Subprocessors used to deliver the Services) adhere to Joint Schedule 11 (Processing Data), Call-Off Schedule 9 (Security) Part A: Short Form Security Requirements), and Appendix A: Departmental Security Standards (**"*Buyer's Security Policy*"**) of the Call-Off Contract.

6.2. In the event that the Supplier may need to deliver Services at DfE office(s), all Supplier Staff would require baseline personnel security standard (BPSS) clearance.

7. SOCIAL VALUE

7.1. Procurement Policy Note PPN 06/20 – taking account of social value in the award of central government contracts, launched a model to deliver social value through government's commercial activities. Potential Providers should demonstrate how they can deliver against the identified social value priority within their response to 'Quality Questionnaire – Mobile V&DS 2025 – itt_3369'.

8. ECONOMIC AND FINANCIAL STANDING (EFS) CHECKS

8.1. DfE are required the assess the EFS of all its suppliers. Potential Providers must complete and return the 'Financial Viability Risk Assessment Tool (FVRAT) – Mobile V&DS 2025 – itt_3369' document by responding within the Technical Envelope section of itt_3369 on Jaggaer.

8.2. DfE has set out the thresholds that Potential Providers must meet and the methodology for assessment within the appropriate table within Appendix C – Further Competition Questionnaire.

8.3. DfE will focus on three (3) key thresholds within the FVRAT to determine a Potential Provider's financial standing. If applicable, the supplementary information in mitigation of any amber or red metrics will be required for the thresholds detailed below:

8.3.1. Turnover

8.3.2. Operational Gross Margin

8.3.3. Acid Ratio

8.4. Although Potential Providers must return a completed copy of the 'Financial Viability Risk Assessment Tool (FVRAT) – Mobile V&DS 2025 – itt_3369' document, it should be noted that the FVRAT will only be assessed in the event that the Potential Provider achieves the highest score following evaluation and is identified as the preferred Supplier. The Supplier must 'pass' the FVRAT assessment in order to be awarded the Contract.

APPENDIX C – FURTHER COMPETITION QUESTIONNAIRE

1. INTRODUCTION

1.1. Appendix C sets out the questions that will be evaluated as part of this Further Competition.

1.2. The following information has been provided in relation to each question (where applicable):

1.2.1. **Weighting** – highlights the relative importance of the question;

1.2.2. **Guidance** – sets out the information for the Potential Provider to consider when preparing a response; and,

1.2.3. **Marking Scheme** – details the marks available to evaluators during evaluation.

2. DOCUMENT COMPLETION

2.1. Potential Providers **must** provide a response to every question within the 'Quality Questionnaire – Mobile V&DS 2025 – itt_3369' document.

2.2. Potential Providers **must** provide a response to all requested cost elements within the 'Pricing Schedule – Mobile V&DS 2025 – itt_3369' document.

2.3. Potential Providers **must** complete the 'Tender Declaration/Supplier Information' and 'Pass/Fail Questionnaire' sections outlined within Jaggaer. Potential Providers **must** 'pass' the Pass/Fail Questionnaire section to be included within the evaluation process.

2.4. Potential Providers **must** also return a completed copy of the Financial Viability Risk Assessment (FVRAT), with financial information from their organisation, parent organisation(s), and subcontractors (as applicable). Potential Providers should be aware that the FVRAT will only be assessed in the event that the Potential Provider achieves the highest score and is identified as the preferred Supplier. Potential Providers **must '**pass' the FVRAT assessment in order to be awarded the Contract.

2.5. Potential Providers **must not** alter/amend the format of any documentation issued as part of this ITT when making a Call-Off Tender response (unless specifically requested), and **must** only submit the information requested by the Authority within this ITT.

2.6. All responses must be made within the Technical Envelope and Commercial Envelope sections within Jaggaer, as applicable.

3. RESPONSE TEMPLATE

3.1. The response templates for each question can be found in the attachments section of itt_3369 on Jaggaer.

3.2. For the avoidance of doubt, in the event that a Potential Provider scores '0' in any of the Quality Questionnaire questions, their Call-Off Tender will be deemed **non-compliant**, and they will be unable to be considered for this requirement.

1	TENDER DECLARATION/SUPPLIER INFORMATION	Not Scored 0%
Guidance:		

The Potential Provider must complete the Tender Declaration and Supplier Information questions by responding within the Technical Envelope section of itt_3369 on Jaggaer.

2	PASS/FAIL QUESTIONNAIRE	Pass/Fail	
Guidance:			
The following questions are Pass / Fail. If a Potential Provider cannot or is unwilling to answer 'Yes', their Call-Off Tender will be deemed non-compliant, and they will be unable to be considered for this requirement. The Potential Provider should confirm by responding within the Technical Envelope section of itt_3369 on Jaggaer.			
2.1	Please confirm that the MVDS solution that your organisation is offering can be delivered through eSIMs, and that your organisation will be able to complete the deployment of eSIMs and transition End Users to the new tariff by no later than 31st May 2025.	Yes	No
2.2	Please confirm that the MVDS solution that your organisation is offering can provide DfE with a flexible all-inclusive voice and SMS tariff, and a flexible Shared Data Bundle.	Yes	No
2.3	Please confirm that the MVDS solution that your organisation is offering allows for the provision of unlimited data SIMs (either physical SIM or eSIM) that are independent of the Shared Data Bundle.	Yes	No
2.4	Should your organisation be successful, please con-firm that you agree, without caveats or limitations, that all Tender documentation and the Order Form and Joint/Call-Off Schedules (Call-Off Contract) which have been issued alongside this ITT will govern the provision of the Contract.	Yes	No
2.5	As this Contract is for the delivery of ICT related services, DfE requires Potential Providers to be certified under the Cyber Essentials Scheme. Please confirm that your organisation holds one of the following: • Cyber Essentials • Cyber Essentials Plus • Cyber Essentials Alternative (e.g., confirmation to the ISO27001 or the IASME standard, where Cyber Essentials requirements have been included within the scope, and are regarded as holding an equivalent standard to Cyber Essentials)	Yes	No

3	ECONOMIC AND FINANCIAL STANDING (EFS) ASSESSMENT	Pass/Fail

Guidance:

The Authority are required the assess the Economic and Financial Standing (EFS) of all its suppliers. The Authority requires Potential Providers to complete and return the **Financial Viability Risk Assessment Tool (FVRAT) – Mobile V&DS 2025 – itt_3369** document by responding within the Technical Envelope section of itt_3369 on the Jaggaer portal.

To complete the FVRAT, Potential Providers will be required to provide financial in-formation in the templates provided. Further instructions are outlined in the "Bidder Instructions" tab. Potential Providers are required to submit financial information for the previous 3-years. Financial information provided should be for the same three (3) financial years for which company accounts have been published.

The FVRAT will request financial information for the previous 3-years, however, the Authority will only assess the past 2-years for this Contract (given the allocated Contract tiering), unless the additional year further aids the EFS assessment.

The "Bidder Instructions" tab will confirm which worksheets the Potential Provider will be required to complete.

The FVRAT **must** be populated by all organisations within a 'group structure' (e.g., financial accounts information for any immediate and ultimate parent companies of Potential Providers alongside their own). Please note that all amounts should be entered in thousands (£000s). For example, £3million would be entered as £3,000 within the FVRAT.

Any Subcontractor who is responsible for delivering more than 20% of this Contract **must** also provide their organisations financial information within the FVRAT.

Although the FVRAT contains nine (9) financial metrics, DfE will only use the following three (3) metrics within its assessment for this Contract:

- Turnover Ratio
- Operational Gross Margin
- Acid Ratio

The FVRAT will automatically RAG rate the calculations of financial metrics. In the event the FVRAT calculates one or more amber or red ratings, Potential Providers are required to provide supporting statements for those metrics at tabs 4.1 – 4.2c (where applicable).

Where red or amber rated metrics are calculated for two (2) consecutive years, two (2) separate supporting statements, each specific to the relevant financial year shall be provided.

The purpose of the supporting statements to be provided alongside any red or amber rated metric is to provide Potential Providers with the opportunity to explain, to the satisfaction of the Authority, why different risk classifications (i.e., green) for that metric may be more appropriate and what mitigations are in place to reduce the risk that the rating represents.

Potential Providers will pass the EFS assessment where:

- All three (3) key metrics generated by the FVRAT are automatically rated as green; or,
- One or more metrics generated by the FVRAT is red or amber rated, but the supporting statement(s) for all red or amber rated metrics provides additional information that explains why, to the satisfaction of the Authority, notwithstanding the original red or amber rating, that the risk identified by the metric's red or amber rating is mitigated and, therefore, a different risk classification is more appropriate.

Potential Providers must provide all the information required. Potential Providers will fail the EFS assessment if they fail to provide all the necessary information required to complete the assessment.

Potential Providers will also fail the EFS assessment where one or more metrics generated by the FVRAT is red or amber rated, and the supporting statement(s) for one or more red or amber rated metric(s) does not provide sufficient additional information to explain why, to the satisfaction of the Authority, notwithstanding the original red or amber rating, the risk identified by the metric's red or amber rating is mitigated and, therefore, a different risk classification is more appropriate.

The decision to pass a Potential Provider with one or more red or amber metrics will be at the Authority's discretion. The exercise of the Authority's discretion will be based upon the strength of the mitigation provided within the financial information in the FVRAT and the content of the associated support statement(s).

Although Potential Providers must return a completed copy of the **Financial Viability Risk Assessment Tool (FVRAT) – Mobile V&DS 2025 – itt_3369** document, it should be noted that the FVRAT will only be assessed in the event that the Potential Provider achieves the highest score following evaluation and is identified as the preferred Supplier. Potential Providers must 'pass' the FVRAT assessment in order to be awarded the Contract.

4	**QUALITY QUESTIONNAIRE – MOBILE V&DS 2025 – itt_3369**	**Weighting 70%**

Guidance:

In order to provide the required information, the Potential Provider should complete and return the **Quality Questionnaire – Mobile V&DS 2025 – itt_3369** by responding within the Technical Envelope section of itt_3369 on the Jaggaer portal.

Question:

Quality Questionnaire – Mobile V&DS 2025 – itt_3369. This section contains six (6) questions, with the following weighting applied: • Q1 – Deployment of eSIMs and transition to new tariff – 20% • Q2 – Flexible Data Bundle – 10% • Q3 – Self-Service Management Portal – 10% • Q4 – Management of User Data – 10% • Q5 – Quality and Contract / Service Management – 10% • Q6 – Social Value – 10% • **Total – 70%**	**Weighting: 100% of 70%**

Marking Scheme:

0 (0%)	The Potential Provider has failed to address the question, submitted a nil response or any element of the response gives cause for major concern that requirements will not be met.
1 (20%)	The Potential Provider has provided a minimal response addressing some of the requirement with very little detail. The response provided does not provide full confidence that the requirements can be met.
2 (40%)	The Potential Provider has provided an acceptable response addressing some of the requirement with partial detail. There are a few concerns about whether the requirements can be met, which requires further clarification.
3 (60%)	The Potential Provider has provided a satisfactory response addressing most of the requirements in sufficient detail, providing confidence that most

	requirements can be met.
4 (80%)	The Potential Provider has provided a strong response addressing most of the requirements in detail, providing confidence that the requirements can be met in full.
5 (100%)	The Potential Provider has provided a thorough response, addressing all requirements in extensive detail, providing confidence that the requirements can be met in full, with added value solutions.

5	**PRICE QUESTIONNAIRE – PRICING SCHEDULE – MOBILE V&DS 2025 – itt_3369**	**Weighting 30%**

Guidance:

Please provide pricing by completing and returning the **Pricing Schedule – Mobile V&DS 2025 – itt_3369** document, by responding within the Commercial Envelope section of itt_3369 on Jaggaer.

All prices shall be in GBP and exclusive of VAT.

Question:

Price Questionnaire – Pricing Schedule – Mobile V&DS 2025 – itt_3369	**Weighting: 100% of 30%**

Marking Scheme:

The maximum mark available for Price will be 30. This mark will be awarded to the lowest priced Potential Provider. Remaining Potential Providers will receive a mark out of this maximum mark on a pro rata basis dependent on how far they deviate from the lowest price.

The calculation that will be used to determine marks is as follows:

$$\text{Score} = \frac{\text{Lowest Tender Price}}{\text{Tender Price}} \times 30 \text{ (maximum mark available)}$$

RM6261 Call-Off Schedule 24 (Supplier-Furnished Terms)

PART 1A: Non-COTS Third Party Software

Not applicable.

PART 1B: COTS Software

Not applicable.

Annex 1: Non-COTS third party software licence terms

Not applicable.

Annex 2: COTS software licence terms

Not applicable.

Schedule 16 (Buyer Specific Security Requirements)

1. Definitions

1.1. In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

"BPSS" **"Baseline Personnel Security Standard"**	the Government's HMG Baseline Personal Security Standard. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" **"Certified Cyber Security Consultancy"**	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" **"Certified Professional"**	is a NCSC scheme in consultation with government, industry, and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"Cyber Essentials" **"Cyber Essentials Plus"**	Cyber Essentials is the government backed industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme, the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body

“Data” **“Data Controller”** **“Data Protection Officer”** **“Data Processor”** **“Personal Data”** **“Personal Data requiring Sensitive Processing”** **“Data Subject”, “Process” and “Processing”**	shall have the meanings given to those terms by the Data Protection Legislation
"Buyer’s Data" **“Buyer’s Information”**	is any data or information owned or retained to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images, or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical, or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Buyer; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Buyer is the Data Controller;
“Departmental Security Requirements”	the Buyer’s security policy or any standards, procedures, process, or specification for security that the Supplier is required to deliver.
“Digital Marketplace / G-Cloud”	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
“End User Devices”	the personal computer or consumer devices that store or process information.
“Good Industry Standard” **“Industry Good Standard”**	the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight, and timeliness as would be expected from a leading company within the relevant industry or business sector.

"GSC" **"GSCP"**	the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	Her Majesty's Government
"ICT"	Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.
"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check (ITSHC)" **"IT Health Check (ITHC)"** **"Penetration Testing"**	an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that ICT system.
"Need-to-Know"	the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"NCSC"	the National Cyber Security Centre (NCSC) is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
"OFFICIAL" **"OFFICIAL-SENSITIVE"**	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP). the term 'OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen,

	or published in the media, as described in the GSCP.
"RBAC" **"Role Based Access Control"**	Role Based Access Control, a method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" **"SAN"**	an information storage system typically presenting block-based storage (i.e., disks or virtual disks) over a network interface rather than using physically connected storage.
Secure by Design Principles	the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/.
"Secure Sanitisation"	the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction-0
"Security and Information Risk Advisor" **"CCP SIRA"** **"SIRA"**	the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"Senior Information Risk Owner" **"SIRO"**	the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This

	includes its executive agencies, arm's length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SPF" **"HMG Security Policy Framework"**	the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently, and securely. https://www.gov.uk/government/publications/security-policy-framework
"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 the Contract.

Operative Provisions

1.1. The Supplier shall be aware of and comply with the relevant HMG security policy framework, NCSC guidelines and where applicable these Departmental Security Requirements which include but are not constrained to the following paragraphs.

1.2. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of Procurement Policy Note: Updates to the Cyber Essentials Scheme (PDF) - Action Note 09/23 dated September 2023, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved and will retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the Services supplied to, or on behalf of, the Buyer.

1.3. Where paragraph 1.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the Services supplied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

1.4. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer's Data being handled in the course of providing the Services

and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).

1.5. Buyer's Data being handled while providing an ICT solution or service must be separated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required in line with paragraph 1.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

1.6. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the products or Services, and that store or process Buyer's Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g., door access), CCTV, alarm systems, etc.

1.6.1. Where remote working is allowed, the Supplier shall have an appropriate remote working policy in place for any Supplier staff that will have access to the Buyer's data and/or systems.

1.7. The Supplier shall have in place, implement, and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Buyer's Data. This policy should include appropriate segregation of duties and if applicable role-based access controls (RBAC). User credentials that give access to Buyer's Data or systems shall be considered to be sensitive data and must be protected accordingly.

1.8. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to:

1.8.1. physical security controls;

1.8.2. good industry standard policies and processes;

1.8.3. malware protection;

1.8.4. boundary access controls including firewalls, application gateways, etc;

1.8.5. maintenance and use of fully supported software packages in accordance with vendor recommendations;

1.8.6. use of secure device configuration and builds;

1.8.7. software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

1.8.8. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;

1.8.9. any services provided to the Buyer must capture audit logs for security events in an electronic format at the application, service and system level to meet the Buyer's logging and auditing requirements, plus logs shall be :

1.8.9.1. retained and protected from tampering for a minimum period of six months.

1.8.9.2. made available to the Buyer on request. These situations might occur when incident investigations are required.

1.9. The Supplier shall ensure that any Buyer's Data (including email) transmitted over any public network (including the Internet, mobile networks, or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.

1.10. The Supplier shall ensure that any Buyer's Data which resides on a mobile, removable, or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer except where the Buyer has given its prior written consent to an alternative arrangement.

1.11. The Supplier shall ensure that any device which is used to process Buyer's Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

1.12. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer's Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

1.13. When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer's Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

1.14. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier's assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier's organisation in line with paragraph 1.15.

1.15. In the event of termination, equipment failure or obsolescence, all Buyer's Data and Buyer's Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC-approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-

contractor protects) the Buyer's Information and Buyer's Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

1.16. Access by Supplier Staff to Buyer's Data, including user credentials, shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Buyer. All Supplier Staff must complete this process before access to Buyer's Data is permitted. [Any Supplier Staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact].

1.17. All Supplier Staff who handle Buyer's Data shall have annual awareness training in protecting information.

1.18. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency, or crisis to the Services delivered. If an ISO 22301 certificate is not available, the supplier will provide evidence of the effectiveness of their ISO 22301 conformant business continuity arrangements and processes including IT disaster recovery plans and procedures. This must include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

1.19. Any suspected or actual breach of the confidentiality, integrity, or availability of Buyer's Data, including user credentials, used or handled while providing the Services shall be recorded as a Security Incident. This includes any non-compliance with the Departmental Security Requirements and these provisions, or other security standards pertaining to the solution.

Security Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery and followed up in writing. If Security Incident reporting has been delayed by more than 24 hours, the Supplier should provide an explanation about the delay. Regular updates on the Security Incident shall be provided to the Buyer in writing until the incident is resolved.

Security Incidents shall be reported through the Buyer's nominated system or service owner.

Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

1.20. The Supplier shall ensure that any Supplier ICT systems and hosting environments that are used to handle, store or process Buyer's Data, including Supplier ICT connected to Supplier ICT systems used to handle, store or process Buyer's Data,

shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. On request by the Buyer, the findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required, to be determined by the Buyer upon review of the ITHC findings.

1.21. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process, or store Buyer's Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.

1.22. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services annually, within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the Services being supplied and the Supplier's, and any sub-contractors', compliance with the paragraphs contained in this Schedule. We note that the Supplier shall allow any auditor access to the Supplier premises as set out in Call-off Schedule 6 (ICT Services) Paragraph 7.1, so long as such access will not: (a) interfere with the interests of Supplier's other customers, and (b) cause the Supplier to breach its confidentiality obligations with its other customers, suppliers or any other organisation.

1.23. The Supplier and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the Buyer through the life of the contract. This will include obtaining any necessary professional security resources required to support the Supplier's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

1.24. Where the Supplier is delivering an ICT solution to the Buyer they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Buyer's Policy. The Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer's expectation is that the Supplier shall provide written evidence of:

1.24.1. implementation of the foundational set of cyber defence safeguards from the Center for Internet Security Critical Security Controls (CIS CSC v8).

1.24.2. any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification issued by an organisation accredited by the United Kingdom Accreditation Service.

1.24.3. any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

1.24.4. documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and

submitted. The Supplier shall provide details of who the awarding body or organisation will be, and date expected.

1.24.5. compliance with the principles of Secure by Design as described at Secure by Design Principles - UK Government Security and, where requested by the Buyer, completion of the table in Appendix 1 (*Secure by Design Principles Evaluation Table*).

Additional information and evidence to that listed above may be required to ensure compliance with DfE security requirements as part of the DfE security assurance process. Where a request for evidence or information is made by the Buyer, the Supplier will acknowledge the request within 5 working days and either provide the information within that timeframe, or, if that is not possible, provide a date when the information will be provided to the Buyer. In any case, the Supplier must respond to information requests from the Buyer needed to support the security assurance process promptly and without undue delay.

1.25. The Supplier shall contractually enforce all these Departmental Security Requirements onto any third-party suppliers, sub-contractors or partners who will have access to the Buyer's Data in the course of providing the Services, before access to the data is provided or permitted.

1.26. The Supplier shall comply with the NCSC's social media guidance: how to use social media safely for any web and social media-based communications. In addition, any Communications Plan deliverable must include a risk assessment relating to the use of web and social media channels for the programme, including controls and mitigations to be applied and how the NCSC social media guidance will be complied with. The Supplier shall implement the necessary controls and mitigations within the plan and regularly review and update the risk assessment throughout the contract period. The Buyer shall have the right to review the risks within the plan and approve the controls and mitigations to be implemented, including requiring the Supplier to implement any additional reasonable controls to ensure risks are managed within the Buyer's risk appetite.

1.27. Any Supplier ICT system used to handle, store, or process the Buyer's Data, including any Supplier ICT systems connected to systems that handle, store, or process the Buyer's Data, must have in place protective monitoring at a level that is commensurate with the security risks posed to those systems and the data held. The Supplier shall provide evidence to the Buyer upon request of the protective monitoring arrangements in place needed to assess compliance with this requirement.

1.28. Where the Supplier is using Artificial Intelligence (AI) and/or Machine Learning (ML) in the delivery of their service to the Buyer, this shall comply with the NCSC's machine learning principles and guidelines for secure AI system development.

Appendix 1 – Secure by Design Principles Evaluation Table

1 Completion of Principles Evaluation Table

1.1 If requested by the Buyer, the Supplier must complete the table in this Appendix 1 (*Secure by Design Principles Evaluation Table*).

1.2 In completing this table, the Supplier must set out how it and any sub-contractors will meet the Secure by Design Principles.

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Principle 1 Create responsibility for cyber security risk Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities.	The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract.	
	The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical infrastructure during their delivery.	
	The Supplier provides adequate and appropriately qualified resources to support the Buyer with following the government Secure by Design approach as part of service delivery. These resources must be reviewed at the beginning of each of the delivery	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	phases during the delivery lifecycle of the service as agreed with the Buyer.	
Principle 2 Source secure technology products Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.	The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance associated with the product and are subject to agreement with the Buyer.	
	The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Buyer's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Buyer should be informed and asked to accept the risk associated with using the product.	
	The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Buyer. Where the product doesn't meet the required obligations, the Supplier must discuss with the Buyer the residual	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	risks associated with using the product.	
Principle 3 Adopt a risk-driven approach Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape.	As provided by the Buyer, the Supplier should share the risk appetite across the supplier's delivery team from the outset.	
	The Supplier supports the Buyer with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery.	
	The Supplier supports the Buyer with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions. During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service.	
	The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	The Supplier factors in the legal and regulatory requirements provided by the Buyer in the risk management process and service design and build.	
Principle 4 Design usable security controls Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand.	The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service.	
	The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls.	
Principle 5 Build in detect and respond security Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response capabilities. These must be continually tested and iterated.	The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the service.	
	The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	service resilience or similar documentation.	
	The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems.	
Principle 6 Design flexible architectures Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities.	As agreed with the Buyer, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats and vulnerabilities.	
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 7 Minimise the attack surface Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security risks while achieving its intended use.	The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Buyer.	
	The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Buyer's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	vulnerabilities that potential attackers can exploit.	
	The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle.	
Principle 8 Defend in depth Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome.	The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service.	
	The Supplier responsible for building the digital service implements security measures to incorporate segmentation.	