

Crown Commercial Service

**Call-Off Order Form for RM6187 Management
Consultancy Framework Three (MCF3)**

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

Order Form

Call-off reference: C97701

The buyer: The Health and Social Care Information Centre (known as NHS Digital)

Buyer address: 7 and 8 Wellington Place, Leeds, West Yorkshire, LS1 4AP

The supplier: Ernst and Young LLP
Supplier address: 1 More London Place London SE1 2AF, United Kingdom

Registration number: OC300001

Sid4gov id:

Applicable framework contract

This Order Form is for the provision of the Call-Off Deliverables and dated

28/07/2022

It is issued under the Framework Contract with the reference number RM6187 for the provision of management consultancy services.

Call-off lot: 3

Call-off incorporated terms

The following documents are incorporated into this Call-Off Contract. Where schedules are missing, those schedules are not part of the agreement and cannot be used. If the documents conflict, the following order of precedence applies:

- This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
- Joint Schedule 1(Definitions and Interpretation) RM6187

- c) The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- a) Joint Schedule 1 (Definitions)
- b) Joint Schedule 2 (Variation Form)
- c) Joint Schedule 3 (Insurance Requirements)
- d) Joint Schedule 4 (Commercially Sensitive Information)
- e) Joint Schedule 6 (Key Subcontractors)
- f) Joint Schedule 7 (Financial Difficulties)
- g) Joint Schedule 10 (Rectification Plan)
- h) Joint Schedule 11 (Processing Data)

Call-Off Schedules

- i) Call-Off Schedule 5 (Pricing Details)
- j) Call-Off Schedule 6 (ICT Services)
- k) Call-Off Schedule 7 (Key Supplier Staff)
- l) Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- m) Call-Off Schedule 9 (Security) Part A
- n) Call-Off Schedule 10 (Exit Management)
- o) Call-Off Schedule 15 (Call-Off Contract Management)
- p) Call-Off Schedule 20 (Call-Off Specification)

- d) CCS Core Terms (version 3.0.7)
- e) Joint Schedule 5 (Corporate Social Responsibility)
- f) 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
- g) Any Statement of Work entered into pursuant to the terms of this Call-Off Contract.

Supplier terms are not 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:

Only the Buyer may insert, revise or supplement Core Terms, Joint Schedules, Call Off Schedules.

1. Definitions

- 1.1 In these Special Terms, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Contractor	means any individual delivering the Services (or any part of them);
CSR Laws	means Laws relating to corporate social responsibility issues (e.g. anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity), including but not limited to the Modern Slavery Act 2015, the Public Services (Social Value) Act 2012, the Public Contracts Regulations 2015 (as amended) and Article 6 of the Energy Efficiency Directive 2012/27/EU, from time to time in force;
CSR Policies	means the Buyer's policies, including, without limitation, anti-bribery and corruption, health and safety, the environmental and sustainable development, equality and diversity, and any similar policy notified to the Supplier by the Buyer from time to time, and "CSR Policy" shall mean any one of them;
Intermediary	means any "intermediary" (as defined in section 61M ITEPA) in respect of which any of Conditions A – C within section 61N ITEPA are met;
ITEPA	Income Tax (Earnings and Pensions) Act 2003;
Medical Devices	means any Deliverable that falls under the definition of a Medical Device in accordance with guidance published by the Medicines and Healthcare Products Regulatory Agency;
Off-Payroll Working Rules	means the provisions of Chapter 10 of Part 2 ITEPA relating to the engagement of workers through intermediaries and the provisions of Social Security Contributions (Intermediaries) Regulations 2000/727 (or, in each case, any other provisions under any law having like effect);
Restricted Staff	any person employed or engaged by either Party, in the capacity of director or in any research, technical, IT, security, engineering, procurement, financial, legal or managerial role who has been engaged in the provision of the Deliverables or management of the Contract either as principal, agent, employee, independent contractor or in any other form of employment or engagement over the previous 12 months, directly worked with or had any material dealings, but shall not include any person employed or engaged in an administrative, clerical, manual or secretarial capacity;
Statement of Work, SOW, or Work Package	means the detailed plan, agreed in accordance with Appendix 1 of this Order Form, describing the Services and/ or Deliverables to be provided by the Supplier, the timetable for their performance and the

	related matters listed in the template statement of work set out in Appendix 1 of the Order Form.
Status Determination	means a status determination pursuant to, and for the purposes of, the Off-Payroll Working Rules;
Tax	means income tax, employee national insurance contributions and employer national insurance contributions (in each case whether or not required to be accounted for under the PAYE rules of the United Kingdom) and any equivalent tax, contribution or similar obligations elsewhere, together, in each case, with all related penalties and interest; and
Third Party Body	has the meaning given to it in Special Term The Supplier shall, if requested by the Buyer, provide such management information as is provided under this Contract to another Buyer or to any Central Government Body, whose role it is to analyse such management information in accordance with UK government policy (to include, without limitation, for the purposes of analysing public sector expenditure and planning future procurement activities) (" Third Party Body "). The Supplier confirms and agrees that the Buyer may itself provide the Third Party Body with management information relating to the Deliverables, any payments made under this Contract, and any other information relevant to the operation of this Contract.

2. IR35

- 2.1 The parties hereby confirm their understanding that the Services are to be provided in a fully contracted-out manner and that, in respect of any individual involved in the provision of the Services (or any part of them) who is not an employee or equity partner of the Supplier, the Supplier shall be the client for the purposes of the Off-Payroll Working Rules and shall therefore be responsible for assessing the tax status of such individuals and preparing a Status Determination.
- 2.2 Subject to Special Term 2.3, the Supplier warrants and undertakes to the Buyer that (i) no Contractor will be (directly or indirectly) engaged via an Intermediary for the purposes of and when delivering the Services (or any part of them) and (ii) all required Tax shall be withheld, deducted and/or accounted for in respect of any payments or other benefits provided to each Contractor.
- 2.3 In circumstances where it is intended that any Contractor is or will be delivering their services (directly or indirectly) through an Intermediary, the Supplier

warrants and undertakes to the Buyer that, prior to the commencement of the delivery of the Services (or any part of them) by that Contractor, the Supplier will:

- 2.3.1 give written notice to the Buyer; and
- 2.3.2 in respect of that Contractor accurately complete a Status Determination and provide to the Buyer a PDF copy of the Status Determination statement for its information (but, for the avoidance of doubt, the Buyer shall not be bound by such Status Determination and can carry out, and follow, its own Status Determination in circumstances where (notwithstanding Special Term 2.1) the Buyer is the client for the purposes of the Off-Payroll Working Rules),

and the Supplier shall procure that such Contractor shall not deliver the Services (or any part of them) without the prior written consent of the Buyer.

- 2.4 Promptly upon request from the Buyer, the Supplier shall provide (or procure provision) to the Buyer of all such evidence, information and assistance as the Buyer reasonably requires in order to confirm that the warranties and undertakings given by the Supplier in Special Terms 2.2 and 2.3 are, and remain, true, accurate and correct in all respects.
- 2.5 The Supplier warrants and undertakes to the Buyer that it shall immediately inform the Buyer if, at any time, it becomes aware of any new or additional fact, matter or circumstance, or any change in any fact, matter or circumstance, in each case, from which it appears that (a) the Off-Payroll Working Rules could apply or (b) any change may need to be made to any Status Determination previously carried out, in each case in relation to the provision of the Services (or any part of them) and / or to any arrangements involving the performance of any services by any Contractor.
- 2.6 The Supplier shall, at all times, comply with any and all requirements or obligations it may have as a result of or in connection with the application of the Off-Payroll Working Rules to the provision of the Services (or any part of them) and / or to any arrangements involving the performance of any services by any Contractor, including, but not limited, to any obligation to make any deductions for Tax, and shall procure the compliance of all other parties involved (directly or indirectly) in the supply of the Services (or any part of them).
- 2.7 The Supplier shall indemnify the Buyer, on demand and on an after-Tax basis, against:
 - 2.7.1 any and all proceedings, claims or demands by any third party (including, but without limitation, HM Revenue & Customs and any successor, equivalent or related body);

- 2.7.2 any and all Tax and any other liabilities, losses, deductions, contributions or assessments; and
- 2.7.3 any and all reasonable costs or expenses and any penalties, fines or interest incurred or payable,

In each case, which arise as a result of, in consequence of, or otherwise in connection with, (i) the Supplier, at any time, being in breach of any of the warranties or undertakings given in Special Terms 2.2, 2.3 and/ or 2.9 and/or (ii) the application of the Off-Payroll Working Rules to the provision of the Services (or any part of them) and / or to any arrangements involving the performance of any services by any Contractor.

- 2.8 The Buyer may at its option satisfy the indemnity given under Special Term 2.7 (in whole or in part) by way of deduction from payments due to the Supplier.
- 2.9 The Supplier warrants to the Buyer that it is not, nor will it prior to the cessation of this Contract become, a "managed service company", within the meaning of section 61B of the Income Tax (Earnings and Pensions) Act 2003.

3. Additional Warranties

- 3.1 The Supplier represents and undertakes to the Buyer that all Deliverables will meet the Buyer's acceptance criteria as defined within the Work Package.
- 3.2 If and to the extent the Services and/ or the Deliverables constitute a Medical Device, the Supplier undertakes and warrants that it has or shall procure all consents, registrations, approvals, licences and permissions relating to Medical Devices as recommended or stipulated by any materials published by the Medicines and Healthcare Products Regulatory Agency.

4. Additional Intellectual Property Terms

- 4.1 The Supplier grants to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, assign, sub-license, adapt, commercially exploit or otherwise deal with any of the Supplier's Existing IPR and, unless agreed otherwise in relation to a particular Work Package, any Third Party IPR to the extent necessary to enable the Buyer to obtain the full benefits of ownership of any New IPR. The Supplier shall procure that such licence shall permit subsequent sub-licensees to sub-license the Existing IPR and Third Party IPR on the same terms and subject to the same restrictions as under this paragraph to enable each further subsequent sub-licensee to obtain the full benefits of any New IPR that are sub-licensed to them.
- 4.2 In respect of all Government Data, the Buyer shall be the owner of all such Government Data and any Existing IPR and New IPR in such Government Data and any modifications, updates and amendments in relation to the same. The

Supplier may not assign, license or otherwise deal with any Government Data or IPRs in such Government Data without the Buyer's specific written consent.

- 4.3 The Supplier may only use its Existing IPR or any Third Party IPR in any New IPR if the Buyer has given its written consent in advance.
- 4.4 The Supplier may only use Open Source Software in any New IPR if the Buyer has given its written consent in advance.
- 4.5 The Supplier shall ensure that all New IPR, Existing IPR and, unless agreed otherwise in relation to a particular Work Package, Third Party IPR licensed or assigned to the Buyer is able to be assigned, novated or otherwise transferred to:
 - 4.5.1 any other Central Government Body, NHS England, NHS Improvement, DHSC or any other Central Government Body or any public or 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; or
 - 4.5.2 where expressly agreed in the Work Package any other public or private body.

Notwithstanding the foregoing, the Supplier shall ensure that all Third Party IPR licensed or assigned to the Buyer is able to be assigned, novated or otherwise transferred to NHS England.

- 4.6 Unless otherwise agreed by the Parties in writing, the Supplier shall ensure that all 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 suitable for publication by the Buyer as Open Source and based on Open Standards (where applicable), and the Buyer may, at its sole discretion, publish the same as Open Source.

5. Document and Source Code Management Repository

- 5.1 The Parties shall work together to ensure that there is appropriate IPR asset management. Where the Supplier is working on the Buyer's system the Supplier shall comply with the Buyer's IPR asset management approach and procedures. Where the Supplier is working on the Supplier's system it will ensure that it maintains its IPR asset management procedures in accordance with Good Industry Practice. Records and documentation associated with IPR asset management shall form part of the Deliverables associated with any Specially Written Software or New IPR.

- 5.2 The Supplier shall comply with any reasonable instructions given by the Buyer as to where it will store Documentation and Source Code, both finished and in progress, during the term of this Call-Off Contract, and at what frequency/intervals.
- 5.3 The Supplier shall provide the Buyer with a copy of the IPR asset management information relating to the Deliverables on request by the Buyer, in a standard portable machine readable format.

6. Information Sharing By the Buyer

- 6.1 The Supplier shall, if requested by the Buyer, provide such management information as is provided under this Contract to another Buyer or to any Central Government Body, whose role it is to analyse such management information in accordance with UK government policy (to include, without limitation, for the purposes of analysing public sector expenditure and planning future procurement activities) ("**Third Party Body**"). The Supplier confirms and agrees that the Buyer may itself provide the Third Party Body with management information relating to the Deliverables, any payments made under this Contract, and any other information relevant to the operation of this Contract.
- 6.2 Upon receipt of management information supplied by the Supplier to the Buyer and/or the Third Party Body, or by the Buyer to the Third Party Body, the Parties hereby consent to the Third Party Body and the Buyer:
 - 6.2.1 storing and analysing the management information and producing statistics; and
 - 6.2.2 sharing the management information or any statistics produced using the management information with any other Buyer or Central Government Body.
- 6.3 If the Third Party Body and/or the Buyer shares the management information or any other information provided under Special Term 6.2, any Buyer or Central Government Body receiving the management information shall, where such management information is subject to obligations of confidence under this Contract and such management information is provided direct by the Buyer to such other Buyer or Central Government Body, be informed of the confidential nature of that information by the Buyer and shall be requested by the Buyer not to disclose it to any body that is not a Buyer or Central Government Body (unless required to do so by Law).
- 6.4 Without limitation, the following additional information may be shared by the Buyer with Third Party Bodies subject to the terms of this Special Term Information Sharing By the Buyer:

- 6.4.1 the Buyer's requirements;
- 6.4.2 the Supplier's rate card and summary cost information;
- 6.4.3 the Buyer's spend information; and
- 6.4.4 the Supplier's registration information on the procurement platform used by the Buyer for the purposes of this Call-Off Contract.

7. Data Protection Impact Assessment Delivery and Assistance

- 7.1 Without limitation to the obligations as set out in Joint Schedule 11 (Processing Data) and the Contract, where expressly agreed in the individual Work Packages, the Supplier shall provide a draft DPIA for all Deliverables under the Contract.
- 7.2 Where expressly agreed in the individual Work Packages, the Supplier shall update the DPIA to be complete for the agreed Deliverables and meeting all Law, prior to the Buyer's Approval of the Deliverable. The Supplier shall be responsible for updating the DPIA at each material change of the Deliverables (including but not limited to each release of new software) and following any Variation.
- 7.3 As of the Call-Off Start Date, it is accepted there is no Processing of Personal Data involved under this Call-Off Contract. There is an expectation that both Parties will assess the data processing arrangement when the subsequent requirements and the Commissioning Process are finalised. It is agreed that each Party shall be responsible for ensuring compliance with the Data Protection Legislation, in relation to its Processing of any Personal Data under this Call-Off Contract. Should the Data Processing position change, the Parties acknowledge that the only Personal Data which may be shared under this Call-Off Contract will be set out in the data processing table in each individual Work Package (where applicable), in the form provided at Appendix 2, below.

8. Third Party Rights for a Public Sector Data Processing

- 8.1 Further to Clause 19, where in Joint Schedule 11 (Processing Data) there is a third-party public sector Controller listed, the named third party public sector Controller will have CRTPA rights in relation to Data Protection Legislation obligations.
- 8.2 Where the third party public sector Controller wishes to exercise its rights pursuant to Special Term 8.1, the Buyer shall notify the Supplier that the rights are to be exercised.

8.3 The enforcement rights granted by Special Term 8.1 are subject to the following restrictions and qualifications:

8.3.1 the Parties may vary, terminate or rescind the Call-Off Contract without the consent of any third party; and

8.3.2 the Buyer may, as agent or trustee, enforce any term of the Call-Off Contract on behalf of another such relevant third party to whom rights have been granted.

9. Data Protection Indemnity

9.1 The Supplier recognises that the Buyer (where controller) will have obligations to meet in Law in relation to any breach and communication to subjects and the ICO, as well as government obligations as to conduct and transparency. Clause 26.2 to 26.5 inclusive of the Core Terms shall not apply in relation to any confidentiality or data protection indemnity provided by the Supplier including but not limited to Clause 14.8(e) of the Core Terms.

10. Confidentiality

10.1 It is recognised that the Health public sector is subject to National Health Service Act 2006 section 9, and in accordance with that statute does not put in place binding legal contracts.

10.2 In relation to Clause 15.5 of the Core Terms, the Buyer shall only be required to notify any public sector recipient that any confidential information is classed as confidential.

11. Premises

11.1 Where either Party uses the other Party's premises, such Party is liable for all Losses arising from any damage it causes to the premises. Such Party is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

11.2 The Supplier will use the Buyer Premises solely for the Call-Off Contract.

11.3 This clause does not create a tenancy or exclusive right of occupation.

11.4 While on the Buyer Premises, the Supplier will:

11.4.1 ensure the security of the premises;

11.4.2 comply with Buyer requirements for the conduct of personnel;

- 11.4.3 comply with any health and safety measures implemented by the Buyer;
 - 11.4.4 comply with any instructions from the Buyer on any necessary associated safety measures; and
 - 11.4.5 notify the Buyer immediately in the event of any incident occurring on the premises where that incident causes any personal injury or damage to property which could give rise to personal injury.
- 11.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.
- 11.6 All Supplier Equipment brought onto the Buyer Premises will be at the Supplier's risk. Upon termination or expiry of the Call-Off Contract, the Supplier will remove such Supplier Equipment.

12. Audit

- 12.1 The Buyer may Audit the Supplier at any time by giving notice in writing, such notice to set out details of the scope of such Audit and the details of the relevant Auditor.
- 12.2 Further to Clause 6.7 of the Core Terms, the Supplier must provide a copy of its Self Audit Certificate supported by an audit report to the Buyer at the end of each Contract Year.

13. Non-Solicitation of Employees or Contractors

- 13.1 The Supplier recognises that the Buyer invests a considerable amount of time, cost and effort in the recruitment and training of staff in the niche area of ICT health services in the public sector. Furthermore, the necessary recruitment governance activity and security checks result in a long lead time in onboarding new staff. Consequently, the Buyer has a legitimate business interest to prevent the unauthorised solicitation or employment or engagement of Restricted Staff.
- 13.2 In order to protect the legitimate business interests of the Buyer (and in particular the Confidential Information, goodwill and the stable trained workforce of each Party), the Supplier agrees that it shall not for the duration of the Call-Off Contract and for a period of 3 months after termination or expiry of this Call-Off Contract solicit or entice away from the employment or service or engagement of the Buyer any Restricted Staff, other than by means of a national advertising campaign open to all-comers and not specifically targeted at the Restricted Staff. The Supplier shall not be deemed to be in breach of this paragraph 13 where Restricted Staff are engaged in response to applying to a general advertising campaign.

14. Further consequences of Call-Off Contract Expiry or Termination

14.1 In addition to the provisions of Clause 10.6 of the Core Terms, at the end of the Call-Off Contract (howsoever arising), the Supplier must:

14.1.1 immediately return to the Buyer:

14.1.1.1 all copies of Buyer Software and any other software licensed by the Buyer to the Supplier under this Call-Off Contract;

14.1.1.2 any materials created by the Supplier under this Call-Off Contract or work in progress where the IPRs are or will be owned by the Buyer; and

14.1.1.3 all Buyer Assets provided to the Supplier by the Buyer in good working order.

14.1.2 immediately upload any items that are or were due to be uploaded to the repository in accordance with Special Term Document and Source Code Management Repository when this Call-Off Contract was terminated;

14.1.3 ensure that any Government Data returned under Clause 10.6.1(d) is, at the direction of the Buyer, provided to the Buyer and any Replacement Supplier with a complete and uncorrupted version of the Government Data in electronic form in the formats and on media agreed with the Buyer and any Replacement Supplier;

14.1.4 work with the Buyer on any work in progress and ensure an orderly transition of the Services to the Replacement Supplier;

14.1.5 provide all information requested by the Buyer on the provision of the Services so that:

14.1.5.1 the Buyer is able to understand how the Services have been provided; and

14.1.5.2 the Buyer and any Replacement Supplier can conduct due diligence.

14.2 Each Party will return all of the other Party's Confidential Information. Each Party will confirm that it does not retain the other Party's Confidential Information except where the information must be retained by the Party as a legal requirement or where this Call-Off Contract states otherwise.

15. Security of Supplier Personnel

15.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel Security Standard (<https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>), as may be amended or replaced by the Government from time to time.

- 15.2 The Supplier shall agree on a case by case basis which Supplier Personnel roles which require specific government National Security Vetting clearances (such as "SC") including system administrators with privileged access to IT systems which store or process Government Data. The Supplier shall provide and maintain a breakdown of the security clearance held for each Supplier Personnel role and shall work with the Buyer to propose any necessary amendments to these in order to provide the Services.
- 15.3 The Supplier shall prevent Supplier Personnel who have not yet received or are unable to obtain the security clearances required by this paragraph from accessing systems which store, process, or are used to manage Government Data, or from accessing Buyer Premises, except where agreed with the Buyer in writing.
- 15.4 All Supplier Personnel that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually, and the Supplier must be able to demonstrate the completion of the training for all in scope staff.
- 15.5 Where Supplier Personnel are granted the ability to access Government Data or systems holding Government Data, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need such access but remain employed by the Supplier's organisation, their access rights shall be revoked by the close of business on the following Working Day. When staff no longer need such access and they leave the Supplier's organisation, their access rights shall be revoked by the close of business on the same Working Day.

16. Corporate Social Responsibility Conduct and Compliance

- 16.1 The Buyer applies corporate and social responsibility values to its business operations and activities which are consistent with the Government's corporate social responsibility policies, including, without limitation, those policies relating to anti-bribery and corruption, health and safety, the environment and sustainable development, equality and diversity.
- 16.2 The Supplier represents and warrants that it:
- 16.2.1 complies with all CSR Laws;
 - 16.2.2 requires its Sub-Contractors and any person under its control, to comply with all CSR Laws; and
 - 16.2.3 has adopted a written corporate and social responsibility policy that sets out its values for relevant activity and behaviour (including, without limitation, addressing the impact on employees, clients, stakeholders, communities and the environment by the Supplier's business activities).
- 16.3 The Supplier shall notify the Buyer in the event that its corporate and social responsibility policies conflict with, or do not cover the same subject matter in an equivalent level of detail as is in, the CSR Policies.

17. Subcontracts

17.1 The Supplier shall ensure that each material Sub-Contract shall include:

- 17.1.1 a right under the Contracts (Rights of Third Parties) Act 1999 for the Buyer to enforce any provisions under the material Sub-Contract which confer a benefit upon the Buyer;
- 17.1.2 a provision enabling the Buyer to enforce the material SubContract as if it were the Supplier; and
- 17.1.3 obligations no less onerous on the Sub-contractor than those imposed on the Supplier under this Contract. Compliance with obligations by Sub-contractors will be documented, maintained, and be available for review by Buyer security personnel.

18. Execution and Counterparts

18.1 This Contract may be executed in any number of counterparts (including by electronic transmission), each of which when executed shall constitute an original but all counterparts together shall constitute one and the same instrument.

18.2 Execution of this Contract may be carried out in accordance with the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) and the Electronic Communications Act 2000. In the event each Party agrees to sign this Contract by electronic signature (whatever form the electronic signature takes) it is confirmed that this method of signature is as conclusive of each Party's intention to be bound by this Contract as if signed by each Party's manuscript signature. In such situation, this Contract shall be formed on the date on which both Parties have electronically signed the Contract as recorded in the Buyer's electronic contract management system.

SPECIAL TERMS

1. The following new sub-clause shall be inserted at clause 32 of the Core Terms:

32.4 The Supplier may decline to enter into a Statement of Work where doing so would place it in (a) a position of Conflict of Interest, or (b) breach of its professional or regulatory obligations or audit independence rules or regulations.

2 – Clause 15.2 (f) of the Core Terms shall be amended to read as follows:

On a confidential basis, to its statutory or regulatory auditors

3 – Clause 23.2 of the Core Terms shall be amended to read as follows:

The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Central Government Body, public or private sector body which performs the functions of the Relevant Authority. If the Relevant Authority intends to assign, novate or transfer its Contract or any part of it to any other body, it will provide the Supplier with reasonable notice, such notice to include the name of the proposed body to which it intends to assign, novate or transfer to, its obligations under its Contract.

Call-off start date: 27/07/2022

Call-off expiry date: 26/07/2024

Call-off initial period: 24 months

Call-off extension period: up to 12 months in aggregate, on the giving of 3 months' notice by the Buyer

Call-off deliverables: To be agreed at individual Statement of Work/project level, however the future Services and Deliverables will be aligned to Lot 3 Complex and Transformation, as set out below:

Business;
Change management;
Complex programmes;
Digital, technology and cyber;
Finance;
HR;
Organisation and operating model;
Performance transformation;
Procurement and/or supply chain;
Project and programme management;
Strategy and/or policy;
Supplier side services and delivery;
Transformation management.

The Parties acknowledge that these requirements are not fully defined at the point of awarding this Call-Off Contract and will be developed over the term of this Call-Off Contract as several projects ('Future Services'). Future Services will be called off using the Commissioning Process outlined at Appendix 1 to this Call-Off Order Form.

The Buyer is not obliged to request any Future Services. In the event that the Buyer does raise a request for Future Services, the Supplier is required to respond in accordance with the Commissioning Process outlined in Appendix 1 to this Order Form and the Call-Off Contract.

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 are:

£5m exclusive of VAT

Call-off charges

See details in Call Off Schedule 5 (Pricing Details)

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

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
- Benchmarking using Call-Off Schedule 16 (Benchmarking)

Reimbursable expenses

Recoverable as stated in Framework Schedule 3 (Framework Prices) paragraph 4

Payment method

Within 30 days of a valid invoice with the SOW reference number/title of the SOW

Buyer's invoice address

NHS Digital,
T56 payables A125,
Phoenix House,
Topcliffe Lane,
Wakefield,
WF3 1WE

Any queries regarding outstanding payments should be directed to NHS Digital's Accounts Payable section by email at financialaccounts@nhs.net

Invoices should clearly quote the purchase order number, be addressed to NHS Digital, T56 Payables A125, Phoenix House, Topcliffe Lane, Wakefield, WF3 1WE and be sent as a PDF attachment by email to the following email address: sps.apinvoicing@nhs.net (one invoice per PDF) and emails must not exceed 10Mb and quote, 'T56 Invoice Scanning' in subject line or alternatively invoices can be sent via post to the above address.

Buyer's authorised representative

Buyer's security policy

NHS Digital Corporate Security Policy appended at Call-Off Schedule 9

Supplier's authorised representative

Supplier's contract manager

Progress report frequency

As set out in each Statement of Work

Progress meeting frequency

As set out in each Statement of Work

From the Call-Off Contract Start Date, the Operational Board shall meet quarterly via video conferencing.

The Operational Board members for each Party are as follows:

Operational Board will be supported by Fortnightly Contract meetings, with the same

attendees, to review status of live and pipeline projects.

Key staff

[REDACTED]

Key subcontractor(s)

N/A – will be agreed at individual project/work package level

Commercially sensitive information

EY Rate Card

Service credits

Not applicable

Additional insurances

Not applicable

Guarantee

Not applicable

Buyer's environmental and social value policy

NHS Digital Social Value Charter available online at <https://digital.nhs.uk/about-nhs-digital/technology-suppliers/nhs-digital-social-value-charter>

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)

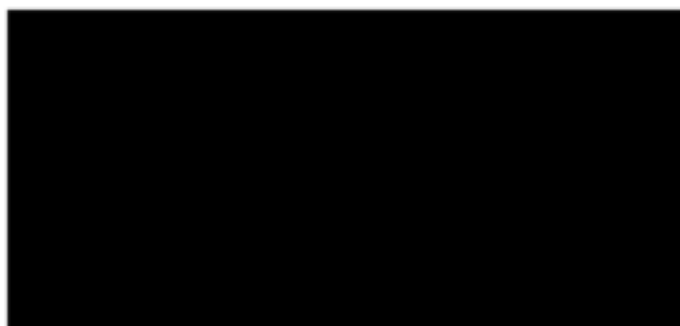
Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

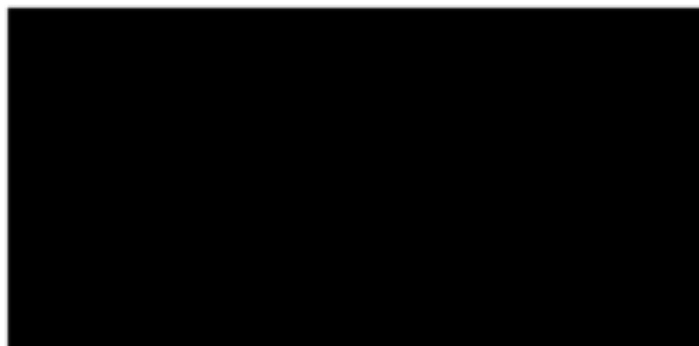
For and on behalf of the Supplier:

Supplier Signature:

A large black rectangular box used to redact the signature of the Supplier.

For and on behalf of the Buyer:

Buyer Signature:

A large black rectangular box used to redact the signature of the Buyer.

APPENDIX 1 – FUTURE SERVICES – COMMISSIONING PROCESS

Future Services will be called off using the Commissioning Process as outlined below:

1. Each future project specific statement of requirements will be coordinated using the commissioning process and the template for future Statements of Work as set out in Appendix 2 of this Order Form.
2. Where the Buyer wishes to commission work under this Call Off Contract, it shall detail the requirements for each individual project including milestones and acceptance criteria ("**Project Requirements**")
 - 2.1 The Buyer's commercial team will communicate Project Requirements to the Supplier whereupon the Supplier shall have five (5) working days (or an alternative period as set out by the Buyer upon communicating the Project Requirements) to respond. All commissioning requests shall be routed through the Commercial department/ dedicated Commercial Leads.
 - 2.2 The Supplier shall respond to the Project Requirements (the "**Supplier's Solution**") using the template Statement of Work. A follow up call to discuss the Project Requirements will be organised with the Project Team if required to walk through the project.
 - 2.3 The Supplier's Solution shall include details of how the work will be undertaken to successfully meet a Project Requirement including milestones, a timeline/activity plan along with CV's (if requested) and a summary of the expertise in the proposed resourcing model, it shall also include a detailed price for the delivery of the Project Requirements in the format provided by the Customer. Where no format is specified, the method used to calculate the price shall be set out in sufficient detail for the Buyer to understand how the price was determined and, as a minimum, the Supplier's pricing will be broken down by the day rates of resources operating on each project and will be no more expensive than the day rates set out in this Contract.
 - 2.4 In most instances, fixed fee or output-based pricing will be used. In other instances, T&M will be utilised based on the submitted rate card. The final decision on the applicable pricing mechanism lies with the Buyer.
 - 2.5 Within five (5) working days of receipt of the Supplier's Solution, including the draft Statement of Work, or in any other period the Buyer deems appropriate, it shall review and feedback comments on the Supplier's Solution and the draft Statement of Work.
 - 2.6 Within two (2) working days of the Buyer providing this feedback (or an alternative period as set out by the Buyer upon communicating its feedback) the Supplier shall provide a final Statement of Work to the Buyer.
 - 2.7 Should either the Buyer or Supplier wish to discuss and/or clarify any aspects of a Project Requirement after the Supplier has submitted its proposed Solution, they shall arrange a call to discuss which may result in the Supplier submitting a further draft for the Buyer's consideration.

- 2.8 Following the Buyer's internal approval process and when the Buyer agrees with the Supplier's Solution, the Buyer shall notify the Supplier that the Statement of Work may be signed and returned to the Buyer for countersigning. Upon countersignature by the Buyer, the Supplier shall commence delivery of the Services detailed in the Statement of Work at the time agreed in the Statement of Work.
3. Amendments to Statement of Work (and associated pricing) after its execution shall follow the Variation process set out at Clause 24 of the Core Terms of the Call-Off Contract.
4. Each Statement of Work shall be part of this Call-Off Contract and shall not form a separate contract to it.
5. At any point during or before the Commissioning Process, the Buyer may seek alternative means of delivering the requirement including potentially re-competing the requirement.
6. The Call-Off Contract is non-exclusive, and the Buyer makes no minimum commitment as to the Services to be purchased under this Call-Off Contract.
- 7. REPORTING AND GOVERNANCE**
- 7.1 Prior to each Operational Board meeting, the Supplier shall provide to the Buyer the following information:
- 7.1.1 Progress reports against Milestones, KPIs and deliverables set out in each Project Requirement detailing Milestone's due for completion that have been achieved, have not been achieved (with accompanying explanations) and any proposed changes to future Milestone dates (with accompanying explanations and impact assessment);
- 7.1.2 Details of the risks and issues associated with future Milestones, KPIs and deliverables and details of actions being taken by the Supplier to remedy those risks and issues;
- 7.1.3 Burn rates of resources (if requested) and any variance against the resource profile set out in the Statement of Work for each project and communicating to the Buyer when discounts will be applicable (in line with the pricing matrix);
- 7.1.4 Any additional reporting requirements as set out in individual Statements of Work being delivered at that time.
- 7.2 On the 3rd week of every calendar month, the Supplier shall provide the Buyer with financial updates against each Statement of Work to help facilitate forecasted accruals, if requested.
- 8. CONTINUOUS IMPROVEMENT**
- 8.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Call-Off Contract duration.
- 8.2 The Supplier should present new ways of working to the Buyer during quarterly Contract review meetings.

- 8.3 Changes to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed prior to any changes being implemented.

9. SUSTAINABILITY AND ENVIRONMENTAL

- 9.1 The Supplier shall possess and operate policies and working practices which encourage a positive approach to sustainability and environmental considerations.
- 9.2 This may include, though need not be limited to:
- 9.2.1 remote working where possible;
 - 9.2.2 telephone and/or video conferencing as an alternative to face-to-face meetings;
 - 9.2.3 travel avoidance;
 - 9.2.4 use and circulation of electronic documents rather than printed documents;
 - 9.2.5 keeping printing to a minimum and use of single colour as opposed to full colour.

10. PAYMENT

10.1 Managing Public Money – Principles

NHS Digital have the responsibility to exercise proper stewardship of public funds, including compliance with the principles laid out in Managing Public Money. The standards ensure we are responsible for establishing and maintaining internal audit arrangements in accordance with the Public Sector Internal Audit Standards and have effective quality internal governance and sound financial management that demonstrates value for money.

11 STATEMENT OF WORK PRICING

- 11.1 The majority of Statement of Work will be fixed fee or output-based pricing where payment will be made upon either the achievement of:
- 11.1.1 Individual Milestones as detailed in each Statement of Work; or
 - 11.1.2 all Milestones detailed in the Statement of Work.
- 11.2 T&M may be utilised based on the submitted rate card.
- 11.3 The final decision on the appropriate pricing model for the Statement of Work shall lie with the Buyer.
- 11.4 Pricing for Statement of Work will be determined during the Commissioning Process and shall be based on the Supplier's rate card set out in this Call-Off Contract.
- 11.5 Payment will only be made if each applicable invoice includes a detailed elemental breakdown of work completed and the associated costs against either an individual milestone or for the entire Statement of Work. As a minimum, the invoice:

11.5.1 Must include appropriate reference and subject title of the Statement of Work; and

11.5.2 Be supported by a copy of the deliverables/sign off criteria from the Buyer in the template provided, dated and signed by the individual nominated Programme Lead(s) that all deliverables have been fully met. The sign-off criteria for milestones/deliverables will be agreed in the Commissioning Process.

12 BASE LOCATION

- 12.1 The base location of where the Services will be carried out at will be at the Buyer's Leeds and/or London offices or provided remotely. This will be confirmed during the Commissioning Process for each requirement.
- 12.2 The Supplier shall, where possible and practical, seek to work from their own locations or home and avoid travel wherever possible as per the sustainability and environmental considerations in paragraph 8 above.

APPENDIX 2 TEMPLATE FOR FUTURE STATEMENT OF WORKS.

Project specific statement of requirements

Ref xxxx Accessing Professional Services: Business Support Services ("Call-Off Contract")

Health and Social Care Information Centre (known as NHS Digital) ("Customer")

and

XXX ("Supplier")

Date of this Statement of Work:	XX/XX/202X
Start Date:	XX/XX/202X
Expiry date:	XX/XX/202X
Statement of Work Reference:	XXX
Call Off Contract Reference:	XXX
Will personal data be shared in the completion of this Statement of Work?	Yes/No If no, then no further actions required, if yes, where required by the Buyer a Data Protection Impact Assessment (DPIA) will need to be completed and the correct terms from Joint Schedule 11 (Processing Data) that apply to be referenced.
Are there any sub-contractors being used to deliver this Statement of Work? [Guidance Note: If a subcontractor is being used, the parties should consider if this subcontractor should be included as a monitored company for the purposes of Joint Schedule 7. If the subcontractor is a monitored company, the credit rating score will need to be included within Annex 2 of Joint Schedule 7.]	Yes/No
Will any Supplier or Third Party IPR be utilised in this engagement?	Yes/ No
Is there the need to exceed the standard liability cap in the completion of this Statement of Work?	Yes/No

Does this work need to start prior to contracts being signed?

Yes/No

Unless otherwise explicitly specified in this Statement of Work, the terms of the Call-Off Contract shall apply to the scope of Services and/or Deliverables set out in this Statement of Work unamended. Unless otherwise specified, changes made to the terms of this Call-Off Contract set out herein only apply to the scope of Services and/or Deliverables as set out in this Statement of Work.

The parties agree that upon signature by both parties, this Statement of Work forms part of the Call-Off Contract as referenced above.

1. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

1.1

2. DEFINITIONS AND ACRONYMS

For the purpose of this Statement of Work, the following words and acronyms shall have the following meanings:

Definition or Acronym	Meaning
-----------------------	---------

3. THE REQUIREMENT

3.1

4. KEY ACTIVITIES, MILESTONES AND DELIVERABLES

Task	Activities	Supplier/Buyer	Detail of Buyer Activities	Outputs
1.				
2.				

Deliverable ID	Deliverable Title	Description	Format
D01			
D02			
D03			

5. BUYER'S RESPONSIBILITIES

6. REPORTING

7. ACCREDITATION

8. STAFF AND CUSTOMER SERVICE

8.1 The engagement is expected to run for approximately [xx] weeks commencing on [xx Month 20xx] and is anticipated to conclude on [xx Month 20xx].

8.2 Any change to the timetable of the engagement outlined in this SOW will be agreed between the parties via the change process set out below.

8.3 The following resources will be provided by the Supplier for the duration of the SOW. If for any reason it is necessary to change the composition of the team, the Supplier will advise the Buyer as soon as possible and endeavour to offer a replacement member with suitable skills and experience.

Role	Name	Grade	Number of days	Rate	Fee

The Supplier's fee is a fixed price of (£xx,xxx) exclusive of VAT. (Payment of expenses under this Call-Off Contract are not allowable.) This has been calculated based on the resource rates set out in Call-Off Schedule 5 (Pricing) of the Call-Off Contract.

9. SERVICE LEVELS AND PERFORMANCE

The Buyer will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA description	Target
1			

10. SECURITY REQUIREMENTS

10.1

11. PAYMENT

11.1 As per the Call-Off Contract, the Buyer shall pay the Supplier the charges within 30 days of receipt of a valid invoice.

11.2 This document sets out the maximum extent of the Buyer's requirements and deliverables/outputs at the time of drafting, and against which the Supplier has provided a costed delivery proposal.

11.3 NHS Digital will discuss with the Supplier the work required over such notice period and pay the Supplier for the appropriate number of chargeable days up to and including the early end date.

12. LOCATION

The Supplier shall provide the Services at the base location detailed within the Call-Off Contract. **[Guidance Note: this should be updated for each SOV/ as applicable]**

13. CHANGE PROCESS

In the event of a change being required to this Statement of Work, the Parties will follow Clause 24 (Changing the contract) of the Call-Off Terms.

14. TERMINATION WITHOUT CAUSE

The Buyer shall have the right to terminate this Statement of Work at any time by issuing a Termination Notice to the Supplier giving at least five (5) Working Days written notice.

15. PROCESSING PERSONAL DATA

The Supplier shall be entitled to Process the Personal Data set out in the table below, in accordance with the terms of the Call-Off Contract:

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 10 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>a) <i>[insert the scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority]</i></p> <p>The Supplier is Controller and the Relevant Authority is Processor</p> <p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data:</p> <p>b) <i>[insert the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier]</i></p> <p>The Parties are Joint Controllers</p> <p>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <p>c) <i>[insert the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]</i></p> <p>The Parties are Independent Controllers of Personal Data</p> <p>The Parties acknowledge that they are independent Controllers for the purposes of the Data Protection Legislation in respect of:</p>

	<p>d) Business contact details of Supplier Personnel for which the Supplier is the Controller,</p> <ul style="list-style-type: none"> 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, [Insert] the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority} <p>[Guidance] where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified)</p>
Duration of the Processing	<i>[Clearly set out the duration of the Processing including dates]</i>
Nature and purposes of the Processing	<p><i>[Please be as specific as possible, but make sure that you cover all intended purposes.</i></p> <p><i>The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i></p>
Type of Personal Data	<i>[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]</i>
Categories of Data Subject	<i>[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]</i>

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 Approved Subprocessors	<i>[Describe how long the data will be retained for, how it be returned or destroyed]</i> [Guidance Note: Any use of a subprocessor will require Buyer approval]
Jurisdiction of Processing	UK [Guidance Note: Any processing outside of the UK will require Buyer approval]

16. INTELLECTUAL PROPERTY RIGHTS

As per Clause 9 (Intellectual Property Rights) of the Call-Off Terms and Special Term 4 (Additional Intellectual Terms) set out in the Order Form, the Supplier shall not acquire any right, title, or interest in or to the Intellectual Property Rights of the Buyer or its licensors, including the:

- (i) Buyer's Existing IPR;
- (ii) Government Data; and
- (iii) New IPRs.

For and on behalf of the Supplier

Name	
Job role/title	

Signature	
Date	

For and on behalf of the Buyer

Name	
Job role/title	
Signature	
Date	

Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In each Contract, unless the context otherwise requires:
 - 1.3.1 the singular includes the plural and vice versa;
 - 1.3.2 reference to a gender includes the other gender and the neuter;
 - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or 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 is a reference to (as it has effect from time to time):

1.3.13.1 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

1.3.13.2 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

	<p>proposed or actual variations to them in accordance with the Contract);</p> <p>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 Deliverables;</p> <p>c) verify the Open Book Data;</p> <p>d) verify the Supplier's and each Subcontractor's compliance with the applicable Law;</p> <p>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;</p> <p>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;</p> <p>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;</p> <p>h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;</p> <p>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;</p> <p>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;</p> <p>k) verify the accuracy and completeness of any:</p> <p>(i) Management Information delivered or required by the Framework Contract; or</p> <p>(ii) Financial Report and compliance with Financial Transparency Objectives as specified by the Buyer in the Order Form;</p>
"Auditor"	<p>a) the Buyer's internal and external auditors;</p> <p>b) the Buyer's statutory or regulatory auditors;</p> <p>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;</p> <p>d) HM Treasury or the Cabinet Office;</p>

	<p>e) any party formally appointed by the Buyer to carry out audit or similar review functions; and</p> <p>f) successors or assigns of any of the above;</p>
"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;
"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 as 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);
"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: <ul style="list-style-type: none"> 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 GDPR;
"Core Terms"	CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;
"Costs"	the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables: 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;

	<ul style="list-style-type: none"> iv) car allowances; v) any other contractual employment benefits; vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and ix) reasonable recruitment costs, as agreed with the Buyer; <p>b) 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;</p> <p>c) 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</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;</p> <p>but excluding:</p> <ul style="list-style-type: none"> e) Overhead; f) financing or similar costs; g) 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; h) taxation; i) fines and penalties; j) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and k) 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"	the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of personal data and privacy; (iii) all applicable

	Law about the Processing of personal data and privacy;
"Data Protection Liability Cap"	the amount specified in the Framework Award Form;
"Data Protection Officer"	has the meaning given to it in the GDPR;
"Data Subject"	has the meaning given to it in the GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "Deliver" and "Delivered" shall be construed accordingly;
"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"	the dispute resolution procedure set out in Clause 34 (Resolving

Resolution Procedure"	disputes);
"Documentation"	<p>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:</p> <ul style="list-style-type: none"> a) 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 b) is required by the Supplier in order to provide the Deliverables; and/or c) 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"	<p>the earlier of:</p> <ul style="list-style-type: none"> a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or

	b) 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"	<p>means for the purposes of calculating each Party's annual liability under clause 11.2:</p> <p>a) in the first Contract Year, the Estimated Year 1 Charges; or</p> <p>b) in any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or</p> <p>c) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;</p>
"Exempt Buyer"	<p>a public sector purchaser that is:</p> <p>a) eligible to use the Framework Contract; and</p> <p>b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of:</p> <ul style="list-style-type: none"> 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;
"Financial Reports"	a report by the Supplier to the Buyer that: (a) provides a true and fair reflection of the Costs and Supplier Profit Margin forecast by the Supplier; (b) provides detail a true and fair reflection of the costs and expenses to be incurred by Key Subcontractors (as requested by the Buyer); (c) is in the same software package (Microsoft Excel or Microsoft Word), layout and format as the blank templates which have been issued by the Buyer to the Supplier on or before the Start Date for the purposes of the Contract; and (d) is certified by the Supplier's Chief Financial Officer or Director of Finance;
"Financial Representative"	a reasonably skilled and experienced member of the Supplier Staff who has specific responsibility for preparing, maintaining, facilitating access to, discussing and explaining the records and accounts of everything to do with the Contract (as referred to in Clause 6), Financial Reports and Open Book Data;
"Financial"	(a) the Buyer having a clear analysis of the Costs, Overhead

Transparency Objectives"	<p>recoveries (where relevant), time spent by Supplier Staff in providing the Services and Supplier Profit Margin so that it can understand any payment sought by the Supplier;</p> <p>(b) the Parties being able to understand Costs forecasts and to have confidence that these are based on justifiable numbers and appropriate forecasting techniques;</p> <p>(c) the Parties being able to understand the quantitative impact of any Variations that affect ongoing Costs and identifying how these could be mitigated and/or reflected in the Charges;</p> <p>(d) the Parties being able to review, address issues with and re-forecast progress in relation to the provision of the Services;</p> <p>(e) the Parties challenging each other with ideas for efficiency and improvements; and</p> <p>(f) enabling the Buyer to demonstrate that it is achieving value for money for the tax payer relative to current market prices;</p>
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	<p>any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by the Affected Party, including:</p> <p>a) riots, civil commotion, war or armed conflict;</p> <p>b) acts of terrorism;</p> <p>c) acts of a Central Government Body, local government or regulatory bodies;</p> <p>d) 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;</p>
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;

"Framework Award Form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
"Framework Contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice;
"Framework Contract Period"	the period from the Framework Start Date until the End Date 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 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);
"GDPR"	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; 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 taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form ;

"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: <ul style="list-style-type: none"> 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 Policy"	the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including: <ul style="list-style-type: none"> 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; b) details of the cost of implementing the proposed Variation; c) 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

	<p>expenditure required by either Party and any alteration to the working practices of either Party;</p> <p>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and</p> <p>e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;</p>
"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"	<p>with respect to any person, means:</p> <p>(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:</p> <p>(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</p> <p>(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;</p> <p>(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</p>

	<p>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;</p> <p>(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;</p> <p>(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;</p> <p>(e) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;</p> <p>(f) where that person is a company, a LLP or a partnership:</p> <p>(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;</p> <p>(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;</p> <p>(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</p> <p>(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</p> <p>(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;</p>
"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

	<p>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;</p> <p>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</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction;</p>
"Invoicing Address"	the address to which the Supplier shall invoice the Buyer as specified in the Order Form;
"IPR Claim"	any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies ;
"Joint Controller Agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (<i>Processing Data</i>);
"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"	<p>any Subcontractor:</p> <p>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>b) 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</p> <p>c) 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,</p> <p>and the Supplier shall list all such Key Subcontractors in</p>

	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, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"Losses"	all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "Loss" shall be interpreted accordingly;
"Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
"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: <ul style="list-style-type: none"> 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"	means the form of report set out in the Annex to Framework

"Template"	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"	<p>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</p> <p>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;</p> <p>but shall not include the Supplier's Existing IPR;</p>
"Occasion of Tax Non-Compliance"	<p>where:</p> <ul style="list-style-type: none"> a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of: <ul style="list-style-type: none"> i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle; ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or b) 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 "	<p>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:</p> <ul style="list-style-type: none"> 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; b) operating expenditure relating to the provision of the Deliverables including an analysis showing: <ul style="list-style-type: none"> 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; c) Overheads; d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables; e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis; f) 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; g) 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 h) the actual Costs profile for each Service Period;
"Order"	<p>means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;</p>

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

"Meeting"	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"	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> i. under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii. under legislation or common law concerning fraudulent acts; or iii. defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or d) 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"	<ul style="list-style-type: none"> a) the Supplier's plan (or revised plan) to rectify its breach using the template in Joint Schedule 10 (Rectification Plan) which shall include: b) full details of the Default that has occurred, including a root cause analysis; c) the actual or anticipated effect of the Default; and d) 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 the context requires);
"Reimbursable Expenses"	<p>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:</p> <ul style="list-style-type: none"> 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 b) 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"	<ul style="list-style-type: none"> a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-

	<p>How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);</p> <p>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</p> <p>c) information derived from any of the above;</p>
"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 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: <ul style="list-style-type: none"> 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; c) those premises at which any Supplier Equipment or any part of the Supplier System is located (where any part of the Deliverables provided falls within Call-Off Schedule 6 (ICT Services));
"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: <ul style="list-style-type: none"> 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; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time; d) 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: <ul style="list-style-type: none"> a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Supplier"	the person, firm or company identified in the Framework Award Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
"Supplier's Confidential Information"	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels ; and/or c) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"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;
"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: <ul style="list-style-type: none"> 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"	Intellectual Property Rights owned by a third party which is or

IPR"	will be used by the Supplier for the purpose of providing the Deliverables;
"Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;
"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – (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;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
"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"	8.0 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
"Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

Joint Schedule 2 (Variation Form)

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

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

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete]** as applicable: CCS / Buyer]
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

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

Signature	
Date	
Name (in Capitals)	
Address	

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

Signature	
Date	
Name (in Capitals)	
Address	

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

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

- 1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
- 1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

- 1.2.1 maintained in accordance with Good Industry Practice;
- 1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;
- 1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
- 1.2.4 maintained for at least six (6) years after the End Date.

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

2. How to manage the insurance

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

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

- 2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
- 2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if you aren't insured

- 3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.
- 3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance you must provide

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

5. Making sure you are insured to the required amount

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

6. Cancelled Insurance

- 6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.
- 6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to

cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

- 7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.
- 7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.
- 7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.
- 7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following standard insurance cover from the Framework Start Date in accordance with this Schedule:
 - 1.1 professional indemnity 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);
 - 1.2 public 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); and
 - 1.3 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)

1. What is the Commercially Sensitive Information?
 - 1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
 - 1.2 Where possible, the Parties have sought to identify when any relevant information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
 - 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
	Start Date	EY pricing information is deemed commercially sensitive.	Call-Off Contract Period

Joint Schedule 5 (Corporate Social Responsibility)

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 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 to the Supplier from time to time.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:
- 2.1.1 eliminate discrimination, harassment or victimisation of any kind; and
 - 2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at <https://www.modernslaveryhelpline.org/report> or by telephone on 08000 121 700.

3.1 The Supplier:

- 3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
- 3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

- 3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.
- 3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.
- 3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.
- 3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
- 3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;
- 3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

- 4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter

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. Sustainability

6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

- 1.1 The Supplier is entitled to sub-contract its obligations under the Framework Contract to the Key Subcontractors set out in the Framework Award Form.
- 1.2 The Supplier is entitled to sub-contract its obligations under a Call-Off Contract to Key Subcontractors listed in the Framework Award Form who are specifically nominated in the Order Form.
- 1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a new Key Subcontractor then they will be added to section 18 of the Framework Award Form. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:
 - 1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - 1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - 1.3.3 the proposed Key Subcontractor employs unfit persons.
- 1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:
 - 1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;
 - 1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;
 - 1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;

- 1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected Framework Price over the Framework Contract Period;
 - 1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and
 - 1.4.6 (where applicable) Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.
- 1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:
- 1.5.1 a copy of the proposed Key Sub-Contract; and
 - 1.5.2 any further information reasonably requested by CCS and/or the Buyer.
- 1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:
- 1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;
 - 1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;
 - 1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;
 - 1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;
 - 1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:
 - (a) the data protection requirements set out in Clause 14 (Data protection);
 - (b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);
 - (c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

- (d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and
 - (e) the conduct of audits set out in Clause 6 (Record keeping and reporting);
- 1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and
 - 1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 7 (Financial Difficulties)

1. Definitions

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

"Credit Rating Threshold"	the minimum credit rating level for the Monitored Company as set out in Annex 2
"Financial Distress Event"	<p>the occurrence or one or more of the following events:</p> <ul style="list-style-type: none">a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold;b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Company;d) Monitored Company committing a material breach of covenant to its lenders;e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; orf) any of the following:<ul style="list-style-type: none">i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract;ii) non-payment by the Monitored Company of any financial indebtedness;

	<p>iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or</p> <p>iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company</p> <p>in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;</p>
"Financial Distress Service Continuity Plan"	a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with each Call-Off Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	Supplier or any Key Subcontractor (including any Key Subcontractor included within a Statement of Work)
"Rating Agencies"	the rating agencies listed in Annex 1.

2. When this Schedule applies

- 2.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.
- 2.2 The terms of this Schedule shall survive:
- 2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any Call-Off Contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and
- 2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off-Contract.

3. What happens when your credit rating changes

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

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

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

where:

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

3.4 The Supplier shall:

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

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

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

if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

- 4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.
- 4.2 In the event that a Financial Distress Event arises due to a Key Sub-contractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:
 - 4.2.1 rectify such late or non-payment; or
 - 4.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.
- 4.3 The Supplier shall and shall procure that the other Monitored Companies shall:
 - 4.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and
 - 4.3.2 where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:
 - (a) submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and
 - (b) provide such financial information relating to the Monitored Company as CCS may reasonably require.
- 4.4 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which

shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

- 4.5 If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.
- 4.6 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:
 - 4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;
 - 4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and
 - 4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).
- 4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.4.6.
- 4.8 CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

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

- 5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:
 - 5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

- 5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or
- 5.1.3 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

6. What happens If your credit rating is still good

- 6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:
 - 6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and
 - 6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).



ANNEX 1: RATING AGENCIES



ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (long term)
Supplier	■
Key Subcontractor	As specified in an applicable Statement Work

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 1. 2. 3. 4. [...]	Timescale [date] [date] [date] [date] [date]
Timescale for complete Rectification of Default	[X] Working Days	
Steps taken to prevent recurrence of Default	Steps 1. 2. 3. 4. [...]	Timescale [date] [date] [date] [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 (*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 (*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 (*Processing Personal Data*) unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
 - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) 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 (*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 (*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 (*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. The contact details of the Relevant Authority's Data Protection Officer are: [REDACTED] at nhsdigital.dpo@nhs.net
2. The contact details of the Supplier's Data Protection Officer are: [REDACTED]
3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
4. Any such further instructions shall be incorporated into this Annex.
5. Where Personal Data will be Processed under a Statement of Work, the Statement of Work shall incorporate the applicable instructions in the format set out in this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>a) <i>[Insert the scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority]</i></p> <p>The Supplier is Controller and the Relevant Authority is Processor</p> <p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data:</p> <p>b) <i>[Insert the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier]</i></p> <p>The Parties are Joint Controllers</p>

The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:

- c) **[Insert]** *the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]*

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:

- d) *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,*
 - **[Insert]** *the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority]*

[Guidance] *where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]*

Duration of the Processing	<i>[Clearly set out the duration of the Processing including dates]</i>
Nature and purposes of the Processing	<i>[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available,</i>

	<p>alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</p> <p>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</p>
Type of Personal Data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
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	[Describe how long the data will be retained for, how it be returned or destroyed]
Approved Subprocessors	[Guidance Note: Any use of a subprocessor will require Buyer approval]
Jurisdiction of Processing	UK [Guidance Note: Any processing outside of the UK will require Buyer approval]

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

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

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Deliverables where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the **[Supplier's/Relevant Authority's]** privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

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

2. Undertakings of both Parties

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

- (a) report to the other Party every **[x]** months on:
 - (i) the volume of Data Subject Access Request (or purported Data Subject Access Request(s)) from Data Subjects (or third parties on their behalf);

- (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation; any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (iv) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant time-scales set out in the Data Protection Legislation;
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- (e) request from the Data Subject only the minimum information necessary to provide the Deliverables and treat such extracted information as Confidential Information;
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

- (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
 - (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
 - (h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
 - (j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.
- 2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.
- 3. Data Protection Breach**
- 3.1 Without prejudice to clause 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:
- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
 - (b) all reasonable assistance, including:

- (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
- (ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
- (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
- (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

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

- (a) the nature of the Personal Data Breach;
- (b) the nature of Personal Data affected;
- (c) the categories and number of Data Subjects concerned;
- (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
- (e) measures taken or proposed to be taken to address the Personal Data Breach; and
- (f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

- (a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

- (b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.
- 4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

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

the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

- (b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- (c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

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

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

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

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

8. Termination

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

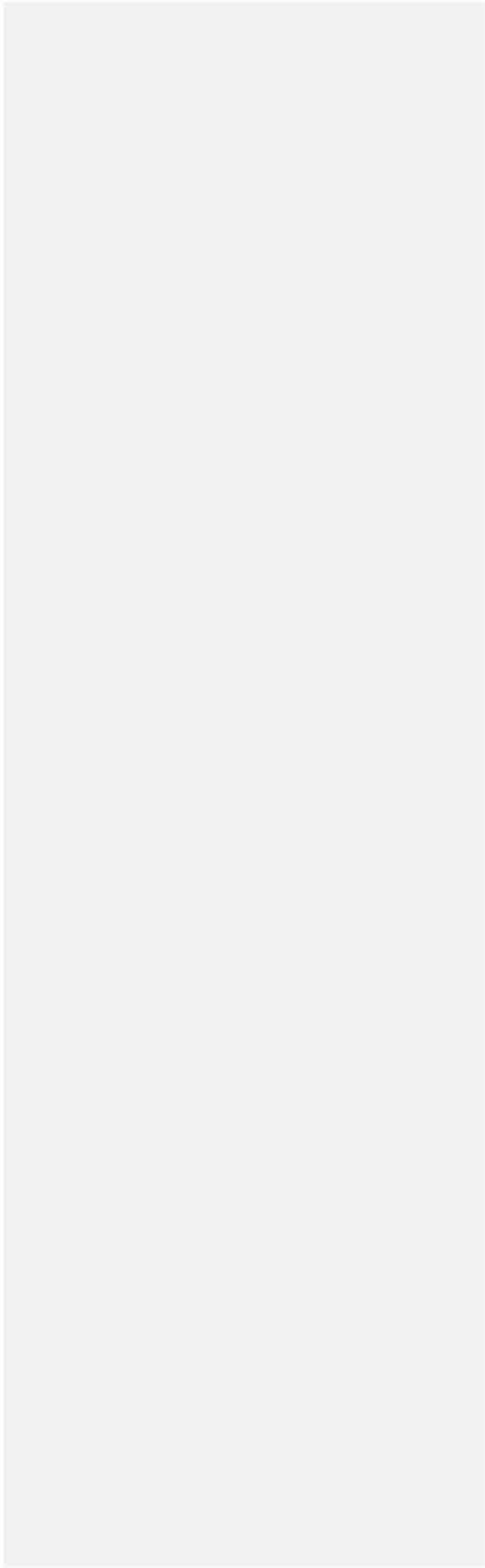
9. Sub-Processing

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

- (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

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



Call-Off Schedule 4 (Call Off Tender)

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
"Defect"	<p>any of the following:</p> <ul style="list-style-type: none">a) any error, damage or defect in the manufacturing of a Deliverable; orb) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; orc) 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 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 the actions needed to remedy each such unsuitable aspect; and
 - 3.2.3 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 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 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 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 (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.

- 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:
- (a) of its own Existing IPR that is not COTS Software;
 - (b) 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 grant 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 9.2.1 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 licensee 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:

- 9.5.3.1 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
- 9.5.3.2 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).

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

2. BCDR Plan

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

- 2.2 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:
- 2.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and
 - 2.2.2 the recovery of the Deliverables in the event of a Disaster
- 2.3 The BCDR Plan shall be divided into three sections:
- 2.3.1 Section 1 which shall set out general principles applicable to the BCDR Plan;
 - 2.3.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and
 - 2.3.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).
- 2.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

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

- 3.1 Section 1 of the BCDR Plan shall:
- 3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
 - 3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
 - 3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
 - 3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
 - 3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

- (a) failure or disruption scenarios and assessments of likely frequency of occurrence;
- (b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
- (c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
- (d) a business impact analysis of different anticipated failures or disruptions;

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Business Continuity (Section 2)

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

- 4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
- 4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

- 4.2 The Business Continuity Plan shall:

- 4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;
- 4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;
- 4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
- 4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

- 5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
- 5.2.1 loss of access to the Buyer Premises;
 - 5.2.2 loss of utilities to the Buyer Premises;

- 5.2.3 loss of the Supplier's helpdesk or CAFM system;
- 5.2.4 loss of a Subcontractor;
- 5.2.5 emergency notification and escalation process;
- 5.2.6 contact lists;
- 5.2.7 staff training and awareness;
- 5.2.8 BCDR Plan testing;
- 5.2.9 post implementation review process;
- 5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
- 5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;
- 5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
- 5.2.13 testing and management arrangements.

6. Review and changing the BCDR Plan

- 6.1 The Supplier shall review the BCDR Plan:
 - 6.1.1 on a regular basis and as a minimum once every six (6) Months;
 - 6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and
 - 6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.
- 6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services

which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

- 6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.
- 6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

- 7.1 The Supplier shall test the BCDR Plan:
- 7.1.1 regularly and in any event not less than once in every Contract Year;
 - 7.1.2 in the event of any major reconfiguration of the Deliverables
 - 7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).
- 7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
- 7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in

any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

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

7.5.1 the outcome of the test;

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

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

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

8. Invoking the BCDR Plan

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

9. Circumstances beyond your control

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

Call-Off Schedule 9 (Security)

Part A (Short Form Security Requirements)

Part A: Short Form Security Requirements

1. Definitions

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

"Breach of Security"	<p>the occurrence of:</p> <p>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</p> <p>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,</p> <p>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;</p>
"Security Management Plan"	<p>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.</p>

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 re-submission, 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.

Annex: NHS Digital Corporate Security Policy



NHS Digital Information Security Policy

Status	Final	
Document Record ID Key	TBC	
Version	1.0	Date: 01/02/2020
Director Responsible	[REDACTED]	
Contact	[REDACTED]	
Author	[REDACTED]	
Next Review Date	01/03/2022	

Contents

1. Background	191
1.1. What is the NHS Digital Information Security Policy?	191
1.2. Why does NHS Digital need an Information Security Policy?	191
1.3. Who does the Information Security Policy apply to?	191
2. Purpose	191
3. Scope	191
4. Mandate	192
5. Accountabilities and Responsibilities	192
5.1. Senior Information Risk Owner (SIRO)	192
5.2. Chief Information Security Officer (CISO)	192
5.3. Data Security Centre Associate Director	192
5.4. Data Protection Officer	193
5.5. Information Asset Owners (IAO)	193
5.6. All Staff	193
6. Governance	194
7. Policy Suite Structure	194
7.1. Strategy	194
7.2. Principles	195
7.3. Policies	195
7.4. Reference Architectures	195
7.5. Standards	195
7.6. Patterns	195
8. Waivers	195
9. Compliance	195
10. Review and Updates	196
11. Document Management	196
11.1. Revision History	196
11.2. Reviewers	196
11.3. Approvals	196
11.4. Related Documents	197

1. Background

1.1. What is the NHS Digital Information Security Policy?

The Information Security Policy is a suite of documents that sets out how NHS Digital and its delivery partners and suppliers manage and protect our information. It explains the responsibilities and accountabilities that various functions, roles and individuals have for ensuring the Confidentiality, Integrity and Availability of information within our organisation.

1.2. Why does NHS Digital need an Information Security Policy?

Having an Information Security Policy helps assure the quality, safety and security of data and information across NHS Digital. The Information Security Policy sets out the requirements to ensure NHS Digital is resilient to compromise and improves response following attack. This helps to demonstrate to the Health and Social Care sector that NHS Digital is a safe place to process and store their data.

1.3. Who does the Information Security Policy apply to?

This policy applies to all NHS Digital information, networks, information systems, applications, locations and users of those systems, services and resources supplied under contract to it.

2. Purpose

NHS Digital's (trade name for the Health and Social Care Information Centre) role is to improve health and social care in England by putting technology, data and information to work. We provide national technology and information services and are a centre of excellence and leadership in the development and use of technology, data and information. The day-to-day business of NHS Digital involves responsibility for some very large and important data 'assets' as well as technology systems. We must ensure that these 'assets' and systems are managed well, protected securely and that our practices are regularly reviewed to identify and manage any new risks.

NHS Digital has a legal responsibility to properly protect and manage its information assets, as well as all the information made available to it by patients, other health and social care organisations, users of the service and information provided by its employees, contractors and business partners.

3. Scope

This policy applies to all NHS Digital information and information systems¹. For the purpose of this policy, information includes data stored on devices, transmitted across networks, printed out or written on paper, sent out by fax, stored on electronic media or spoken in conversation, or over a communications medium. All information that is collected, created, processed, stored, transmitted (physically or electronically) or destroyed during the course of NHS Digital business activity is an asset of the organisation and as such is governed by this policy.

¹ Information and Information Systems comprise of network devices, servers, databases, applications, data, locations and users of those systems, services and resources supplied by or to NHS Digital.

4. Mandate

The mandate to develop and enforce this policy is delegated from the NHS Digital Board to the Senior Information Risk Owner.

5. Accountabilities and Responsibilities

There are a number of key roles that are accountable and responsible for the successful implementation and ongoing management of Information Security within NHS Digital. The key roles are defined within this section, specific accountabilities and responsibilities are documented within the complete suite of information security policy documents.

5.1. Senior Information Risk Owner (SIRO)

The **SIRO** is accountable for information risk within NHS Digital and advises the Board on the effectiveness of information risk management across the organisation. Operational accountability for Information Security shall be delegated by the SIRO to the Chief Information Security Officer (CISO).

5.2. Chief Information Security Officer (CISO)

The **CISO** is accountable for the definition of the Information Security Policy and its day to day operational effectiveness and other associated artefacts.

The CISO's responsibilities include:

- Leading on the provision of expert advice to the organisation on all matters concerning Information Security, compliance with policies, setting standards and ensuring best practice.
- Providing a central point of contact for Information Security within NHS Digital.
- Ensuring the operational effectiveness of security controls and processes across NHS Digital and all the services NHS Digital provides to the wider Health and Social Care system.
- Monitoring and co-ordinating the operation of how the organisation manages its security provisions the (Information Security Management System).
- Being accountable to the SIRO and other bodies for Information Security across NHS Digital.
- Monitoring potential and actual security events and incidents with appropriate expert security resource across NHS Digital and the wider Health and Social Care system.
- Leading the response to major cyber incidents across NHS Digital and the wider Health and Social Care system.
- Providing advice and expertise to the wide Health and Social Care system on security threats.
- Providing Assurance on the security posture at NHS Digital.

5.3. Data Security Centre Associate Director

The Data Security Centre **Associate Director** is responsible for the implementation, monitoring and operation of the Information Security Policy.

The Associate Director's responsibilities include:

- Leading the operation of the National Cyber Security Operations Centre
- Developing and delivering an integrated Information and Cyber Security strategy and roadmap for NHS Digital, while ensuring that NHS Digital's staff and stakeholders are assured of the security and safety of systems and processes.

- Embedding strong security policy and governance across NHS Digital technology teams to ensure programmes deliver securely and ongoing BAU security governance to ensure NHS Digital are applying security policies and standards.
- Driving technology security architecture, innovation and design.
Lead the implementation of nationally focussed information and cyber security programmes of work to deliver new, innovative and high quality security capabilities across the Care system. To act as Deputy Risk Owner (SIRO) as and when required by the NHS Digital SIRO. Data Protection Officer (DPO).

5.4. Data Protection Officer

The **Data Protection Officer (DPO)** is responsible for assisting NHS Digital to monitor its compliance with the General Data Protection Regulation (GDPR); the Data Protection Act 2018 and NHS Digital's own policies in relation to the protection of personal data. The tasks of the Data Protection Officer as set out in GDPR Article 39 are:

- to inform and advise NHS Digital of its obligations in relation to GDPR and the Data Protection Act 2018.
- to monitor NHS Digital's compliance with GDPR; the Data Protection Act 2018 and NHS Digital's own policies in relation to the protection of personal data.
- to provide advice on Data Protection Impact Assessments (DPIAs) and monitor their performance
- to co-operate with the ICO
- to be a contact point for data subjects with regard to all issues related to the processing of their personal data and the exercise of their rights.

5.5. Information Asset Owners (IAO)

All **Information Asset Owners** are individually responsible for ensuring that this policy and its dependant policies are managed and maintained in their business area. This includes:

- IAOs ensure that all users of information or information systems within the business area are aware, trained and comply with this policy.
- IAOs ensures that access to systems, information or physical assets is appropriately authorised, monitored and reviewed.
- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks.
- Supporting personal accountability of users within the business area(s) for information security.
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

5.6. All Staff

All Staff are responsible for Information Security and remain accountable for their individual actions in relation to NHS Digital information and information systems. Staff are defined as all NHS Digital employees and third party staff (eg consultants, contractors, temporary

employees, work package resources). Staff should ensure that they understand their role and responsibilities, and that failure to comply with this policy and its dependant policies may result in disciplinary action. In particular, all staff should understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information.
- How to report a suspected security incident.
- Their responsibility for raising any Information Security concerns with the Information Security Officer in line with the Risk and Issue Management Policy.

6. Governance

This policy is owned by the CISO.

The Cyber Design Authority (CDA) will ensure that the policy and its associated artefacts are reviewed and approved on a regular basis and will create new artefacts as required.

Information security risks which exceed the accepted threshold in the NHS Digital Risk Appetite Statement will be escalated to the CISO as part of the normal operations and from there to the Executive Management Team (EMT) as appropriate. Any exceptional risks or issues will be escalated directly to the SIRO by the CISO.

7. Policy Suite Structure

The Information Security Policy is made up of a suite of artefacts that provide a different purpose, there is also a hierarchy to these documents as shown in the diagram below.

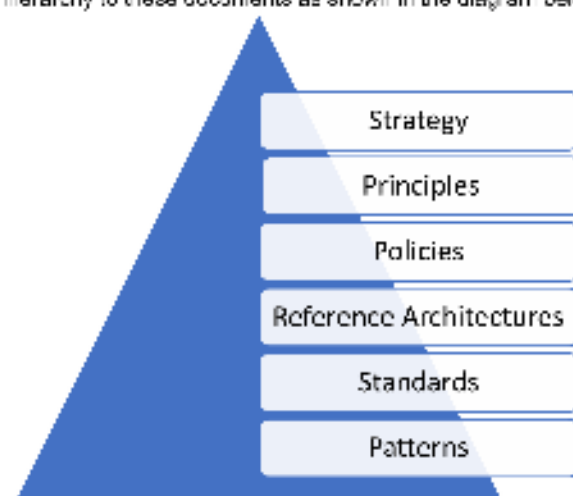


Figure 1: CDA artefact hierarchy

7.1. Strategy

The strategy sets out the medium (3-5 years) to long term (5-10 years) vision for the department.

7.2. Principles

The security principles are rarely changing guidelines that inform and support the design and definition of cyber security within NHS Digital.

7.3. Policies

The policy suite is a series of documents which define the rules, as set out in the strategy, which must be followed.

7.4. Reference Architectures

Reference architectures are conceptual models of security that describe required security capabilities. They are technology agnostic and do not describe implementation details.

7.5. Standards

Standards are the minimum technical baselines that systems must adhere to meet Cyber Security policies and principles.

7.6. Patterns

Patterns are reusable designs that can be used for a number of different projects and systems. These will feed from the standards and define what requirements are appropriate for different systems.

8. Waivers

In the policies the term **"shall"** is used to indicate an absolute requirement. Failure to meet these requirements will require a formal waiver:

- Any waivers for new systems or services that cannot meet Information Security Policy **shall** be presented to the Technical Review and Governance Group (TRG). This **shall** be carried out prior to deployment and managed through the design caveats or the waiver process. TRG **shall** inform the Cyber Design Authority of any waivers granted.
- Any waivers for existing systems or services that cannot meet the controls defined in the Information Security Policy **shall** be presented to the Cyber Design Authority.
- Any waivers for processes or procedures that cannot meet Information Security Policy **shall** be submitted to the Cyber Design Authority. This **shall** be carried out prior to deployment and managed through the design caveats or exception process.
- Such waiver requests **may** invoke the Risk Management process in order to clarify the potential impact of any deviation to the controls detailed in this policy.
- Waivers for policies and standards **shall** be maintained in accordance with the NHS Digital Risk Management Framework for accountability, traceability and security governance reporting to senior management.

9. Compliance

Compliance with this policy **shall** occur as follows:

Compliance	Due Date
New systems or processes	From the first day of approval

Existing systems or processes	Within 6 months of the approval of the standard/policy
-------------------------------	--

Compliance with the Information Security Policy suite will be monitored through a number of different methods covering the design, development, go-live, live service and decommissioning of systems and data.

10. Review and Updates

This policy will be reviewed, as a minimum, on an annual basis and updated as needed by the Cyber Design Authority.

11. Document Management

11.1. Revision History

Version	Date	Summary of Changes
0.1	21/06/2019	Initial Draft
0.2	05/07/2019	Updates from [REDACTED]
0.3	18/09/2019	Updates following feedback from [REDACTED]
0.4	19/09/2019	Further updates
0.5	19/09/2019	Updates following review comments from [REDACTED]
0.6	05/11/2019	Addition of [REDACTED]
0.7	21/11/2019	Updated following comments from [REDACTED]
1.0	20/04/2020	Director name change

11.2. Reviewers

11.3. Approvals

11.4. Related Documents

Reference	Title	Location
-----------	-------	----------



NHS Digital Corporate Acceptable Use Policy

Status	Final		
Document Record ID Key	1-4C		
Version	2.0	Date	01/02/2021
Director Responsible	[REDACTED]		
Contact	[REDACTED]		
Author	Corporate Security Team		
Document Classification	OFFICIAL		
Next Review Date	15/04/2022		

Contents

1. Purpose	201
2. Scope	201
3. Target Audience	201
4. Applicability and Responsibility	201
4.1. Applicability	201
4.2. Responsibility	202
4.2.1. All Staff	202
4.2.2. Line Managers	202
4.2.3. Head of Corporate Security	202
4.2.4. Chief Information Security Officer (CISO)	202
4.2.5. Senior Information Risk Owner (SIRO)	202
5. Terminology	202
6. Policy	203
6.1. Policy Principles	203
6.2. General	203
6.3. Management Responsibilities	204
6.4. Acceptable Use & Behaviour Principles	204
6.5. Protective Security Behaviours	204
6.6. Acceptable Use of ICT and User Obligations	205
6.6.1. Principles	205
6.6.2. User Obligations – General Controls	206
6.6.3. Authentication Controls	207
6.6.4. Delegation of Email Access	207
6.6.5. Data Storage	207
6.6.6. Internet Usage	208
6.6.7. Email Usage	209
6.6.8. Mobile Device Usage	209
6.6.9. Instant Messaging (IM) Tool Usage	209
6.6.10. Contact Centre Voice Over IP (VOIP) Phone Usage	210
6.6.11. Cost Control and sustainability	210
6.6.12. Software	210
6.7. Access to Patient Confidential Data	210

6.8. Investigations	211
6.9. Incident Management	211
6.10. Administration Rights	211
6.11. Developer Network	211
6.12. Third Party Extranet Access	211
6.13. Responsibilities for Manager and Recruiting	212
Managers	212
6.13.1. Creating User Accounts	212
6.13.2. Job Roles / Assignments	212
6.13.3. Removing Staff Member Accounts	213
6.13.4. Access to Leavers Information	213
6.13.5. Emergency Access to User Information	214
6.14. Remote Access	214
6.15. User Damage/Lost Equipment	214
6.16. Bring Your Own Device (BYOD)	214
6.17. USB/Removable Media	214
6.18. Governance	215
7. Exceptions	215
8. Compliance	215
9. Review and Updates	216
10. Document Management	216
10.1. Revision History	216
10.2. Approached for Review	216
10.3. Reviewers	216
10.4. Approvals	217
10.5. Related Documents	217
10.6. Definitions	218
Appendix A – User Obligations and Behaviours	218

1. Purpose

The purpose of the NHS Digital Corporate Acceptable Use Policy (AUP) is to detail the acceptable use of not only NHS Digital assets, but the behaviours that shall be observed when interacting with security controls on NHS Digital's estate.

This policy will safeguard and reduce the risk to the organisation from a security incident by all staff who have access NHS Digital's assets, systems, buildings and information, through the instilling of the organisation's security culture, behaviours and awareness.

It is based on the Government Security Function's four dimensions of Protective Security¹ considerations of cyber (CybSec), personnel (PerSec), physical (PhySec) and technical (TecSec) security.

2. Scope

This policy describes Protective Security considerations CybSec, PerSec, PhySec and TecSec around acceptable use of NHS Digital's systems. This includes all information systems, hardware, software and channels of communication, such as voice-telephony, social media, video, email, instant messaging, internet and intranet.

This policy also covers users' personal information which is processed by NHS Digital's equipment. Processing of personal information is further defined in the NHS Digital Acceptable Use of ICT and User Obligations Policy and the NHSmail Acceptable Use Policy. This policy provides guidance on the expected behaviours of all staff with regards to security equipment and controls, which may be encountered when performing day to day duties or responsibilities. This is further expanded upon in the NHS Digital Physical and Environmental Security Policy.

The alignment of this document to the [Government Functional Standard: GovS:007 Security](#), for NHS Digital policy sets out National Cyber Security Centre Cyber Assessment Framework objectives (NCSC-CAF) areas is shown in Appendix A – User Obligations and Behaviours.

3. Target Audience

This Policy is intended for use by:

- All Staff

4. Applicability and Responsibility

4.1. Applicability

The policy is applicable to all NHS Digital employees and third party staff (e.g., consultants, contractors, temporary employees), hereby referred to in this document as All Staff², that use or have access to NHS Digital systems and/or information and those who have access to buildings and places of work on the NHS Digital estate.

² All Staff term will be used to identify that this policy is focused towards but is not limited to NHS Digital Employees, Contractors, Consultants, 3rd Party Suppliers and Visitors.

¹ Protective Security is the organised system of defensive measures instituted, operated and maintained within an organisation including its supply chain, with the aim of achieving and maintaining security.

4.2. Responsibility

4.2.1. All Staff

All Staff **shall** be accountable for ensuring that they too understand their responsibilities as defined in this policy and continue to meet the requirements. If additional support or advice is required in order to meet the requirements of this policy, All Staff **should** first discuss this with their line manager, who will advise on available training.

4.2.2. Line Managers

All managers **shall** support and encourage their teams in the reporting of security incidents and provide the necessary guidance to ensure compliance is managed effectively across the organisation. Additional education and awareness training **should** be available to support line managers and Human Resources colleagues in the application of the policy.

4.2.3. Head of Corporate Security

The NHS Digital Head of Corporate Security **shall** be responsible for the alignment of all security related policies generated by the business, to ensure that the appropriate level of security controls have been adopted based on an assessment of risk and consequences to the business.

4.2.4. Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) **shall** be responsible for producing and approving the NHS Corporate Acceptable Use Policy and ensuring it is adhered to across NHS Digital.

4.2.5. Senior Information Risk Owner (SIRO)

The NHS Digital Senior Information Risk Owner (SIRO) **shall** be accountable for all information risk within NHS Digital.

5. Terminology

Throughout this policy a number of key terms will be referenced, they are 'shall', 'should' and 'may'. The below table provides the definition in relation to the three phrases:

Term	Meaning/Application
Shall	This term is used to state a Mandatory requirement of this Policy
Should	This term is used to state a Recommended requirement of this Policy
May	This term is used to state an Optional requirement

6. Policy

6.1. Policy Principles

This policy will help all staff understand what behaviours, activities, and responsibilities are expected of them, in order to support acceptable and responsible use of systems in NHS Digital. These Policy Principles will be referred to later on in the document.

Policy Principle 1

Acceptable Use is the responsibility of all individuals. **All Staff** of NHS Digital systems shall be aware of their expected behaviours, use systems responsibly, and report suspected breaches of the Acceptable Use Policy.

Policy Principle 2

All Staff shall be aware of the required behaviours relating to CybSec and use NHS Digital systems in a way that maintains the security of systems, data, and other users at all times.

Policy Principle 3

All Staff shall be aware of the required behaviours relating to PerSec and use NHS Digital systems in a way that is professional, respectful, and lawful at all times.

Policy Principle 4

All Staff shall be aware of the required behaviours relating to PhySec and apply recommended physical security controls to the use of NHS Digital systems and assets at all times.

Policy Principle 5

All Staff shall be aware of the required behaviours relating to TecSec and apply secure-by-design principles when considering the application of technical controls and their user interactions.

6.2. General

NHS Digital abides by current relevant legislation, which includes but is not limited to:

- Data Protection Act (DPA) 2018.
- General Data Protection Regulations (GDPR) 2016.
- Human Rights Act (HRA) 1998.
- Regulation of Investigatory Powers Act (RIPA) 2000.

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (TR-LDP) 2000.
- Computer Misuse Act (CMA) 1990.

The use of any NHS Digital system shall be regulated by the NHS Digital Code of Business Conduct Policy.

All NHS Digital's IT systems, services, end-user devices and shared repository areas are for NHS Digital business use and limited personal use only. NHS Digital reserve the right to monitor all activity taking place on their systems. This is in accordance with the DPA and Article 8(2) of the European Convention on Human Rights as incorporated by the HRA.

6.3. Management Responsibilities

All managers within NHS Digital shall be responsible for encouraging and supporting the behaviours as shown at Appendix A. They shall have a key responsibility to lead by example and demonstrate the necessary behaviours at all times.

6.4. Acceptable Use & Behaviour Principles

Policy Principle 1

Acceptable use is the responsibility of all individuals. All staff must be aware of their expected behaviours, use systems responsibly, and report suspected breaches of the Acceptable Use Policy.

All staff shall be responsible for supporting and adhering to the behaviours shown at Appendix A.

The consistent application of the following principles will ensure an effective selection of security controls across all four dimensions of Protective Security, whilst also improving the wider understanding and identification of the appropriate use and behaviour, required by all staff.

6.5. Protective Security Behaviours

All staff shall adhere to a set of principles outlining the acceptable use of NHS Digital's systems, considering security of information, systems and people across the 4 domains of security.

Policy Principle 2

All staff shall be aware of the required behaviours relating to CybSec and use NHS Digital systems in a way that maintains the security of systems, data, and other users at all times.

Policy Principle 3

All staff shall be aware of the required behaviours relating to PerSec and use NHS Digital's systems in a way that is professional, respectful, and lawful at all times.

Policy Principle 4

All staff shall be aware of the required behaviours relating to PhySec and apply recommended physical security controls to the use of NHS Digital's systems and assets at all times.

Policy Principle 5

All staff shall be aware of the required behaviours relating to TecSec and apply secure-by-design principles when considering the application of technical controls and their user interactions.

6.6. Acceptable Use of ICT and User Obligations

This section details the acceptable use of NHS Digital's IT hardware and software. The obligations outlined are designed to protect the organisation and its user community. All staff are required to abide by the terms of this section which is effective from the time you are granted access to our systems, until the termination of your contract with the organisation and the return of all of your provided equipment.

6.6.1. Principles

In order to protect all staff and NHS Digital when using corporate IT equipment for either business or personal purposes and to ensure correct, secure conduct of business and operations, it is mandatory that any use of this equipment complies with the following legislation:

- The General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Digital Economy Act 2017
- Any related legislation

Further, any use of IT equipment must also comply with the following principles:

- It does not risk bringing NHS Digital into disrepute or placing it in a position of liability.
- It does not violate any provision set out in this or any other policy or contravene our standards of conduct.
- It does not cause damage or disruption to our systems or business.

In relation to personal use, the following points underpin the principles outlined in this guidance:

- It does not waste official time or interfere with official duties.
- It does not contravene our policies.
- It does not significantly add to our running costs.
- All points in 4.2 should also be adhered to in relation to personal use

Personal use is not a right and should be exercised with discretion and moderation. NHS Digital does not accept any liability for claims arising out of personal use of its IT facilities. NHS Digital retains the right to:

- Prohibit personal use of IT facilities without warning or consultation either collectively, where evidence points to a risk to the business, or individually, where evidence points to a breach of this or any other organisational policy.
- Monitor the usage of IT facilities for the purposes of protecting its legitimate concerns.

6.6.2. User Obligations – General Controls

Unauthorised access to any of our IT systems or services is forbidden, and you have a duty of care to ensure:

- The prevention of unauthorised, malicious, and illegal access to any of our systems, resources, or materials.
- The prevention of any individual from using any of our IT systems, resources, or materials in order to commit or facilitate an illegal offence or action counter to the organisational policies.
- The prevention of unauthorised, malicious, and illegal modification to, or corruption of any of our IT systems, resources and / or materials.

This includes:

- Proactively sharing account and password details.
- Attempting to use the Internet or email system to receive or transmit pornographic, violent, or sexual images.
- Attempting to use the network or resources to duplicate copyright protected software for personal and / or financial gain.
- Attempting to use the network and / or resources to develop, create or perpetuate any form of computer virus or malicious software, including the purposeful uploading or transmission of a known computer virus or item of malicious software to others, whether internal or external to the organisation.
- Attempting to use security scanning tools on corporate resources and web sites.

You must not personally undertake, and should report immediately any suspicious attempt to subvert, amend, modify, or otherwise inappropriately compromise or affect, any of our IT application systems resources or materials, including:

- Attempting to alter, erase, modify or otherwise compromise, any legitimate software, files, databases, or any other form of stored information that is either owned by, been developed by or on behalf of, NHS Digital or is under the guardianship of NHS Digital without proper and appropriate authority and / or legitimate intent.
- Attempting to copy or move any legitimate software or associated material to any storage medium other than that which it is intended by the organisation.
- Knowingly causing or facilitating damage to any of the NHS Digital IT systems, resources, or materials, including any attempt to cause or damage the reliability of any of NHS Digital's IT application systems, resources or materials.
- Preventing, or otherwise hindering, legitimate electronic access by authorised staff to either NHS Digital's ICT network and application systems, or to any information held within NHS Digital's ICT network and application systems.
- Corrupting, or knowingly attempting to corrupt, the accuracy and completeness of any information held within the Corporate network and application systems.
- Access to any of the organisation's corporate systems/services must be granted by Tech-Services.
- You are required to screen lock your terminals, workstations, laptops, tablets and/or smartphones when the device is not in use, even if it is only for a short period of time.
- All user sessions on laptop devices will timeout and lock after 5 minutes of inactivity. Mobile devices should keep the time out set to 5 minutes or less.

Within NHS Digital offices:

- When not in use laptops/tablets should be stored in a personal locker or carried with NHS Digital employees outside of working hours.

6.6.3. Authentication Controls

The scope of the authentication controls section is the authentication used by NHS Digital on its local Windows (Active Directory) Network. Authentication may be undertaken using the Windows Hello functionality or using a username and password. Tech Services use Microsoft Authenticator for enhanced authentication to sensitive corporate resources. During the initial setup of user accounts, a temporary password may be created. The communication procedures for these temporary passwords shall always ensure the security of passwords. Once issued with a temporary password you must change this when first logging into the system.

You must always operate NHS Digital's equipment using assigned and approved credentials. Passwords must meet complexity requirements and must not be shared with anyone. Logging onto NHS Digital's equipment with credentials that you are not authorised to use is not permitted.

TechServices will set passwords requirements in line with the NHS Digital Password Policy, which is available to review in the Policy Tool.

You are responsible for the security of your credentials and are therefore responsible for all computer transactions that are made with your user ID.

Revealing an account password to others or allowing the use of an account by others is prohibited. This includes family and other household members when working from home. If a password becomes known to another person, it must be changed immediately. For example, passwords must not be shared in order to "cover" for someone out of the office.

We recommend that you do not use the same password for multiple systems as this would increase the security risk if your password is exposed to someone other than yourself. Keeping separate passwords for home and work is strongly recommended.

Repeated failed attempts to authenticate will result in system lockout. If you are locked out, please contact the Service Desk on 0113 516 0000 (option 1).

6.6.4. Delegation of Email Access

You may, at your own discretion, permit other users (i.e. Personal Assistant/Business Support) to access your email. As the email account owner, it is your responsibility to ensure that access is appropriate and does not result in individuals having inappropriate access to sensitive information. It is also your responsibility to remove any inappropriate shared access to your mailbox when you, or they, move assignment or leave the organisation. The sharing of email passwords is not good practice and alternative solutions can be put into place; further advice can be obtained from contacting TechServices via [ResolveIT](#).

6.6.5. Data Storage

All NHS Digital's data **should** be stored in one of the following locations, and not locally on laptop / desktop hardware:

- NHS Digital Shared Data Drive
- NHS Digital SharePoint
- NHS Digital Personal Drive
- NHS Digital OneDrive
- NHS Digital approved removable media

You are not permitted to store personal music/photos on NHS Digital's approved data storage locations.

NHS Digital OneDrive and NHS Digital SharePoint Online are cloud-based solutions

hosted by Microsoft in UK Data Centres. In general, documents classified up to 'OFFICIAL – SENSITIVE' may be stored on these systems (see the [Data Handling and Security Classification Standard](#) for classification definitions). However, you must note that:

- OneDrive is for individual copies of documents or drafts that are work in progress.
- Official records should only be stored on SharePoint Online, as per the NHS Digital Records Management Policy.
- Any storage of Patient Confidential Data and Patient Identifiable Data in cloud-based solutions must be reviewed and approved following the procedures identified in the Public Cloud & Co-location Infrastructure Platforms Policy.

6.6.6. Internet Usage

Access to the Internet is provided to support the business, but it may be used for occasional and reasonable personal use if it does not interfere with the performance of duties and does not conflict with NHS Digital policies.

You must comply with the Copyright, Design and Patents Act, 1988 when downloading material from internet sites.

Instant messages, email, video conferencing and other communications mechanisms made across the Internet may not be secure. Only NHS Digital's authorised communication mechanisms can be used for this.

Transactions are not permitted on sites requiring software to be downloaded before proceeding.

We accept no responsibility for any charges or loss incurred in relation to personal purchases or financial transactions using NHS Digital's IT facilities regardless of cause. Intentionally accessing or forwarding material that is defamatory, pornographic, sexist, racist, related to online gambling or material whose publication is illegal or risks causing offence or dispute to NHS Digital is prohibited. If access to restricted material is required, a request to TechServices with supporting business justification and manager endorsement should be submitted, via eStore using the 'Elevated Internet Browsing Rights' form, prior to attempting to access the material / site.

Access control software is in operation that will block you from entering sites that are deemed inappropriate. Circumventing monitoring controls is not permitted. We reserve the right to amend restrictions and block sites as appropriate.

All internet traffic and sites visited by users is monitored (i.e. the number of times sites have been visited and the volume of data transferred). This uses Secure Socket Layer (SSL) decryption: SSL-encrypted traffic is decrypted, inspected, and then re-encrypted with the proxy certificate before it is relayed to the client. This enables the cloud proxy to serve the correct notification page to you. The following categories are excluded from SSL decryption:

- Financial Data and Services
- Prescribed Medications
- Education
- Government
- Health Websites

SSL decryption is enabled on the internet control service (or internet proxy service); in order to establish a trust between the proxy and the client, a proxy certificate is deployed to all corporate machines. This public and private key for this certificate remains on the internet proxy service. The private key of the certificate is not shared with anyone, a compromise is not possible, and traffic will work like a normal secure connection.

All internet data that is composed, transmitted and/or received by NHS Digital's computer systems, is considered to belong to NHS Digital and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

If you produce, collect and/or process business-related information in the course of your work, the information will remain the property of NHS Digital. This includes such information stored on third-party websites, such as webmail service providers and social networking sites such as, Facebook and LinkedIn.

6.6.7. Email Usage

You must comply with the [terms and conditions of the NHSmail service](#).

NHS Digital emails must not be automatically forwarded to other non-NHS or Government email addresses e.g. Hotmail, Gmail etc.

You **should** be aware that email addresses and content sent via NHSmail or using an NHS Digital device may be inspected without notice if there appears to be a cause to do so.

NHSmail **should** always be used for communications relating to NHS Digital's business. Alternative email may be used if NHSmail is not available or when explicit authorisation has been given by a manager.

You can only connect to NHSmail using home/personal computers using the NHSmail portal (www.nhs.net) and **should** not download any mails/documents to any device which does not have NHS Digital's compliant encryption installed.

6.6.8. Mobile Device Usage

All staff (excluding contractors and work packages) are provided with the option to be issued with a corporate mobile device by TechServices when they join the organisation. All mobile devices issued are intended as a business tool to enable staff to perform their role.

Personal mobile devices can be used for NHS Digital work-related purposes. Please see the [Bring Your Own Device Policy](#) for further information.

Occasional personal use of corporate mobile devices (Voice, SMS, and Data) is permitted. We log all usage of mobile devices and **should** personal usage appear to be excessive this may be investigated further with a view to requiring the member of staff to fund excessive use.

All NHS Digital's corporate mobiles **must** be registered with the NHS Digital Enterprise Mobility Management system. Instructions on how to complete registration are provided to all staff that are issued with a corporate mobile device.

Internet access via NHS Digital's corporate mobiles is subject to the same restrictions as outlined above. Applications may be installed onto smart phones; however, support will not be offered for these applications and should these be suspected of causing issues with core business functionality these applications **must** be removed.

You **must** ensure that all corporate mobiles are always stored securely.

You must not permit unauthorised personnel (such as friends or relatives) to use NHS Digital's corporate IT equipment in your possession.

6.6.9. Instant Messaging (IM) Tool Usage

IM tools are part of the TechServices Desktop build application set, available on all Corporate IT devices, including mobiles and tablets. IM applications are subject to change over time based on the current approved application standards, set by TechServices.

All messages created, sent, or retrieved over IM are the property of NHS Digital and **should** be regarded as publicly available information.

You will receive IT equipment with the approved IM software application pre-installed.

The use of any service, other than the approved IM service, is not permitted as the use of non- corporate solutions is a security risk.

Under no circumstances **should** financial data, confidential files, or any other sensitive,

private, or proprietary information be transferred using IM applications, nor **should** sensitive, private, or proprietary information be discussed using IM applications.

If you think that your IM username or session has been compromised, in or out of core working hours, please shut down your session immediately and call TechServices as soon as possible (you may be required to log a separate security incident). Please contact the Service Desk on 0113 518 0000 (option 1).

If you are using the organisation's IM service, you should ensure that your use of the IM service is ethical and lawful, and nothing is said in an IM session that would risk damage to NHS Digital's reputation.

6.6.10. Contact Centre Voice Over IP (VOIP) Phone Usage

VOIP phones are provided as a business tool to enable specific teams to perform their role (i.e. Contact Centres) or by approved use cases. Personal use of desk phone is permitted, but if the usage appears to be excessive this may be investigated further. NHS Digital logs all desk phone usage. Desk phones should be logged out of when leaving the office.

6.6.11. Cost Control and sustainability

You are expected to ensure public funds are not wasted unnecessarily: this includes:

- Only requesting hardware where a genuine business need exists.
- Advising TechServices if a piece of hardware or software is no longer required.
- Powering down hardware at the end of the working day wherever possible.
- Taking good care of NHS Digital equipment in your care.
- Using IT tools to reduce the need to travel for business wherever possible using collaboration software options.
- Limiting the use of email and its associated carbon footprint through active use of Share-Point over sending attachments and only replying, all where there is a business need.

6.6.12. Software

Where software has specific boundaries of use, this will be clearly articulated on the [Software Request Form](#). Where this is applicable, staff **shall** adhere to the usage permitted.

6.7. Access to Patient Confidential Data

If you have access to Patient Confidential Data, you must adhere to all relevant statutory and organisational requirements. Further information can be found in the NHS Digital Confidentiality Policy.

It is strictly forbidden for you to knowingly access NHS Digital controlled data to browse, search for or look at any information relating to yourself, your own family, friends or other persons, without a legitimate purpose.

Staff are responsible to report any suspicions relating to computer misuse to management that include:

- Attempting to gain access or exceed the access and/or privilege levels to any of NHS Digital's IT application systems, resources, or materials for which you do not have direct authorisation.
- Attempting to use another user's credentials to gain access to any of the NHS Digital's IT application systems, resources, or materials.

6.8. Investigations

It may be necessary for information to be accessed by TechServices or the Privacy, Transparency and Ethics (PTE) team for the purposes of an investigation. This information and documentation may be on media such as:

- Laptops/desktops (including virtual machines on Virtual Desktop Infrastructure (VDI)/tablets).
- Developer Solution based virtual machine.
- Mobile devices including BYOD.
- Email.
- Network drives.
- Issued removable media.
- Cloud storage e.g. OneDrive, SharePoint Online.
- Paper information.
- Instant Messenger.
- Internet browsing history (this will not include the data transferred).

This will only be permitted on the express authorisation of either the Chief People Officer or the SIRO. A formally nominated deputy for either post may also provide authorisation in their absence.

6.9. Incident Management

Any suspected or detected occurrence of a potential breach of information security within NHS Digital, **must** be immediately reported to the National Service Desk on 0300 3035222. This includes lost or stolen hardware (tablet, laptop and/or mobile device). This **must** also be reported to the Service Desk on 0113 518 0000 (option 3) to ensure all equipment is dealt with in line with security procedures.

6.10. Administration Rights

Elevated (local administration) user rights are not permitted on corporate build machines. Authorised developers or other individuals whose role requires the need to utilise elevated rights, subject to completion of the appropriate request process, may be granted access to the TechServices Developer Solution, or if not appropriate, a Developer (DevOps) Laptop. For access to the TechServices Developer Solution please raise a request via eStore, searching for 'PC to PC migration'.

6.11. Developer Network

The Developer Network is a controlled network environment for use by NHS Digital's employees, including temporary staff, contractors and work packages, carrying out development work for NHS Digital. It is available to NHS Digital assets and BYOD devices. It allows controlled access to N3/HSCN, Azure and AWS.

The Developer Network Policy has to be read and agreed to before access to the Developer Network is granted.

For access to the Developer Network please raise a request via the eStore, searching for 'Developer Network'.

6.12. Third Party Extranet Access

For third parties to operate in an efficient manner with NHS Digital it may be necessary

to permit them access to our intranet, SharePoint and/or Teams sites. If you wish for a third party to access the data, the risk **must** be assessed by you and you must put the appropriate controls in place. No data classified as 'Official/Official - Sensitive' is to be placed on externally facing web servers without approval of the relevant Information Asset Owner.

Access to information which is not in the public domain **shall** be controlled by identification and authentication mechanisms which **shall** control access by third parties, subject to prior approval by NHS Digital.

For third parties providing support for Corporate Systems and Services, NHS Digital's Corporate tools are available to allow the specific access that is required. Approval for use and access to these tools is governed and administered by TechServices.

6.13. Responsibilities for Manager and Recruiting

Managers

Managers have a duty to meet the obligations set out for all staff but in addition, they have responsibilities of any NHS Digital's staff they manage (including contractors, secondees and consultants).

6.13.1. Creating User Accounts

A unique identifier will be given to allow staff to accessing NHS Digital's systems. Before access can be gained to our corporate network (and subsequently any computer applications including email, internet and activity databases) authorisation must be obtained from a manager or recruiting manager. The creation of new user accounts is carried out as part of the standard recruitment process.

For access to Spine systems, you are required to complete a Registration Authority (RA) form. Information on this can be found here: [Care Identity Service forms - NHS Digital](#). For this to be accepted this must be approved and counter-signed by the Manager.

The process for allocating the unique identifier must ensure that authentication credentials are always held securely.

When requesting access for a new starter, the manager or recruiting manager is responsible for ensuring that the minimum access that is required for the new staff member to perform their role is requested.

Whilst managers or recruiting managers authorise the business justification for access to systems the Information Asset Owner for specific system(s) also needs to confirm that it is appropriate for the staff member to have access the requested system(s).

The manager or recruiting manager is responsible for communicating to TechServices any changes to a staff member's role or if their access rights need amending. For example, role changes, resignation or termination, maternity leave, sabbaticals, or any other interruptions to continuous employment.

6.13.2. Job Roles / Assignments

All staff have access to the systems and services they require to do their role. This includes shared drives and SharePoint sites, and a range of specialist systems like the Electronic Staff Record, Jira and Power-BI.

To control the information assets appropriately, and to comply with best practice and the new General Data Protection Regulation, access to systems and services is reviewed periodically during assignments and at the end of assignments. Managers have responsibilities for reviewing this at the end of assignments.

Responsibilities for managers, when releasing someone from their assignment:

- Review the assignee's permissions to any shared drives, SharePoint sites or services that your teams use to perform their role.
- Check the Unified Register and update any information assets that the assignee had access to.
- If the assignee is moving within the organisation, request they update their manager in the People Portal.

When a new assignee is due to join your project/team:

- Check what access they need, and request access to any shared drives through ResolveIT.
- Ask your SharePoint Site Administrators to grant any access to any SharePoint or Office365 sites.
- Review any of your services on the Unified Register to enable access to other services - review whether the new assignee's current equipment is suitable for their new assignment. If not, raise a ResolveIT call to have it switched.

When someone you manage changes assignment:

- Work with their previous manager and new manager, reviewing the steps above on permissions and access to services.
- Ask the assignee to update their manager details on the People Portal to reflect their new manager (this will update the intranet and organisation charts in the future).
- This might be necessary because of promotion, starting a secondment out of the organisation, starting a period of maternity or paternity leave, or starting a career break.

When someone you manage is going to leave the organisation:

- Complete a 'leaver notification request' via the People Portal.

Responsibilities for recruiting managers is to strengthen access controls. TechServices will automatically disable accounts and access for temporary workers and contractors where the contract end date has passed. Managers will be prompted in advance of the contract end date and will be responsible for the following:

- When a temporary worker or contractor is coming to the end of their contract, the manager **should** complete a 'Notification of Variation (NoV)' form on eStore as soon as they have agreed an end date.
- When a temporary worker or contractor needs to be extended, a NoV form also needs to be completed.
- If you do not complete a NoV form for the individual prior to their leave date, then access to all NHS Digital IT systems will be disabled on the contract end date.

Please note: if you need to extend a contractor (band 8A and above), you will have to complete a Professional Services Business Case (PSBC) (PSBCs can take between 22 and 80 days for approval).

6.13.3. Removing Staff Member Accounts

Access to all system resources shall be disabled on the day any staff member leaves NHS Digital. This includes the disablement of Active Directory accounts and NHSmail accounts which will be marked as 'leavers' on the NHSmail portal.

On departure the staff will surrender all NHS Digital equipment to TechServices, including but not limited to, computers, iPads, mobile, and encrypted USB sticks.

6.13.4. Access to Leavers Information

The manager **shall** ensure that leavers who depart in a planned manner hand over all NHS Digital information to which they have access to. Access to specific data once a staff member has departed in a planned manner will only be made available with authorisation

from the Chief People Officer or the Senior Information Risk Owner (SIRO).
A formally nominated deputy for either post may also provide authorisation in their absence.

6.13.5. Emergency Access to User Information

There are circumstances where an individual has information stored to which the business needs access to in unforeseen circumstances. In such cases access to specific data will only be made available with authorisation of the Chief People Officer or the Senior Information Risk Owner (SIRO). A formally nominated deputy for either post may also provide authorisation in their absence.

This includes information on:

- PCs, VDI based machine and laptops.
- Smart phones / tablets / mobile devices.
- Email.
- Network drives.
- Cloud storage e.g. OneDrive, SharePoint Online.
- Paper information.

6.14. Remote Access

TechServices supports agile working by providing a remote access service to enable you to connect remotely to the NHS Digital network when you are not at an NHS Digital office location.

When working from home you should ensure that you have the appropriate facilities to support Remote Access to the NHS Digital network (i.e. your own broadband connection).

6.15. User Damage/Lost Equipment

All staff **shall** look after the IT equipment issued to them by TechServices. If your corporate devices get damaged or lost, please contact the Service Desk as soon as possible on 0113 518 0000 (option 1). If your device is lost, TechServices operate a three strike rule, whereby if your equipment is damaged or lost more than three times, it will not be replaced (this will be reset after 3 years). You will be required to move to Bring Your Own Device (BYOD), with VDI as the corporate service, or alternatively TechServices will look to recover the cost from your salary.

6.16. Bring Your Own Device (BYOD)

For policies regarding bringing your own device for use with NHS Digital ICT systems, please refer to the [NHS Digital BYOD Policy](#), which can be viewed on the Policy Tool and the [CDA ISMS SharePoint site](#).

6.17. USB/Removable Media

Removable media could become a source of malware into the NHS Digital network, with the potential for major implications.

Examples of removable media devices include:

- CDs
- DVDs

- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)
- Mobile devices connected via USB used as storage.

To protect the organisation, the use of all types of removable media devices is prohibited, unless the business use is justified and approved. All removable media must be assessed and approved for use by the Information security team.

Requests for removable media must be made by raising a ResolveIT and purchased by NHS Digital.

6.18. Governance

This policy will be reviewed annually, and in accordance with the following, as and when required:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities
- Changes to organisational infrastructure.

7. Exceptions

In this policy and its dependant policies or standards the term "shall" is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below:

- Any exemptions to the application of this policy or where controls cannot be achieved to shall be presented to the Data Security Centre to seek approval, this then may be escalated to the CISO/EMT for further approval.
- Once an exemption has been granted by the review group/governance board it shall be maintained in accordance with the NHS Digital Risk and Issue Management Strategy and Framework for accountability, traceability and security governance.

If you believe that a policy that has been published and approved by the CDA is incorrect, requires further discussion or a new artefact requires inclusion please inform the CDA via the Cybersecurity@nhs.uk mailbox.

8. Compliance

Compliance with this policy shall occur as follows:

Compliance	Due Date
------------	----------

On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard/policy

In addition, NHS Digital contracts of employment require everyone to comply with organisational policies.

9. Review and Updates

This policy will be reviewed on an annual basis and updated as needed by the Corporate Security Team and approved by the Cyber Design Authority (CDA).

10. Document Management

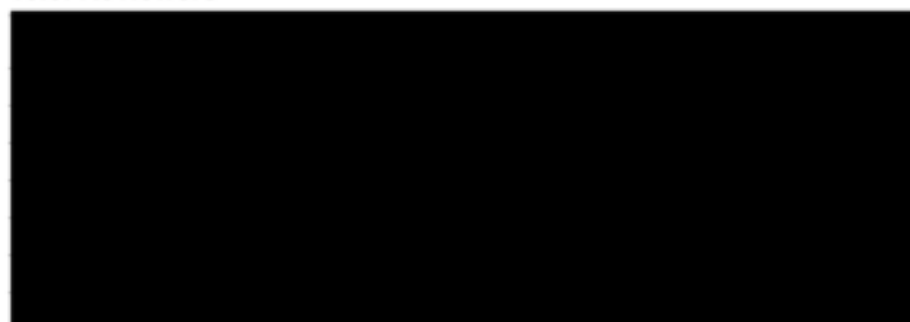
10.1. Revision History

Version	Date	Summary of Changes
1.0	15/07/2020	Approval at CDA Board and published
2.0	11/12/2020	Addition of ICT AUP

10.2. Approached for Review

Reviewer Name	Title/Responsibility	Department	Date

10.3. Reviewers



10.4. Approvals

10.5. Related Documents

Reference	Title	Location
	NHSmail AUP	https://portal.nhs.net/Forms/AcceptablePolicy
	NHS Digital Security Conduct Policy	TBC
	NHS Digital Incident Management Policy	https://nscib365.sharepoint.com/sites/InfoSec/MgtSys/Documents/Incident%20Management/Policy-Information%20Security%20Incident%20Management-v1.2-20200207.docx?d=efda062ad2f8844773bc3386252ca2da4c&csf=1&web=1&e=30u2PIg
	NHS Digital Code of Business Conduct	TBC
	NHS Digital Records and Document Management Policy	TBC
	NHS Digital Social Media Policy	https://nscib365.sharepoint.com/sites/InfoSec/MgtSys/Documents/Personnel/Policy-Social%20Media%20Policy-v1.0-20092020.docx?d=ef556c2f3cf434a46a3ac7b3ac124908fc2&csf=1&web=1&e=60u0f1G
	NHS Digital Physical and Environmental Security Policy	https://nscib365.sharepoint.com/sites/InfoSec/MgtSys/Documents/Physical/Policy-Physical%20and%20Environmental%20Security-v1.2-20200207.docx?d=ef47011f8ca95449c95Ccb762c99d494da&csf=1&web=1&e=60u000G
	NHS Digital ISMS SharePoint site	https://nscib365.sharepoint.com/sites/InfoSec/MgtSys/SecurePages/Welcome.aspx

10.6. Definitions

Reference	Definition
1	"All Staff" term will be used to identify that this policy is focused towards but is not limited to NHS Digital Employees, Contractors, Consultants, 3 rd Party Suppliers and visitors.
2	Protective Security is the organised system of defensive measures instituted, operated and maintained within an organisation including its supply chain, with the aim of achieving and maintaining security.

Appendix A – User Obligations and Behaviours

Behaviour ID	User Obligation or Behaviour to be Observed (Management)
B1	The acceptable use requirements outlined in this Policy shall be clearly articulated to staff.
B2	All Staff shall be provided with access to this Policy. A confirmation of understanding and acceptance should be documented in the appropriate manner (e.g. a physical signature or electronic assent).
B3	Requirements outlined in this Policy should be reviewed regularly and kept in line with current NHS Digital security guidelines.
B4	Account administrators shall be informed when staff leave NHS Digital projects or departments, in order to have their NHS Digital account disabled in accordance with the Joiners, Movers and Leavers Policy and Identity and Access Management Policy.

Behaviour ID	User Obligation or Behaviour to be Observed (Cyber & Technical)
B5	Users shall read and confirm they understand this policy prior to use of NHS Digital equipment, information or facilities. A record should be kept of this agreement, to this AUP and supporting AUPs, understanding that breaching this policy may result in disciplinary procedures.
B6	Users shall apply the NHS Digital Security Classification Policy appropriately to document headers and email subject lines and handle all data and information in a manner appropriate to its security classification.
B7	Users shall use information, systems and equipment in line with NHS Digital's security and Information Management policies (e.g. NHS Digital Security Configuration Policy or NHS Digital's Application Security Policy).
B8	Users shall immediately report any breach of this Acceptable Use Policy and/or supporting AUPs to a line manager and adhere to the NHS Digital Information Security Incident Management Policy when a breach of the policy is suspected or reported.
B9	Information concerning NHS Digital which is not already in the public domain shall not at any time be divulged to any unauthorised person.
B10	Users shall create secure passwords following best practice guidance as detailed in the NHS Digital Password Policy.
B11	Users shall ensure that all information is created, used, shared and disposed of in line with business need and in compliance with the NHS Digital Information Security Management Policy, and Information Asset Inventory guidance.
B12	Users shall not use personal or non-NHS Digital supplied removable media with NHS devices or systems, unless in exceptional circumstances where there is a documented business need and with the prior approval of the Corporate Security Team.
B13	Users shall not attempt to access personal data including patient data unless there is a valid business need this is appropriate to their role.
B14	Users shall not attempt to access, amend, damage, delete or disseminate another person's files, emails, communications or data without the appropriate authority.
B15	Users shall not download software onto NHS Digital devices, with the exception of NHS Digital devices where software has been permitted from an official source, appropriately licensed, and does not compromise the performance or security of the device.

Behaviour ID	User Obligation or Behaviour to be Observed (Personnel & Physical)
B16	Users should undertake available education and awareness training on security controls necessary to protect NHS Digital's information and assets.
B17	Users shall understand that they and NHS Digital have a legal responsibility to protect personal and sensitive information.

Behaviour ID	User Obligation or Behaviour to be Observed (Personnel & Physical)
B18	Users shall understand that both business and personal use will be monitored as appropriate.
B19	Users shall protect usernames, staff numbers, smart cards and passwords appropriately.
B20	Users shall comply with the requirement to return equipment and assets upon leaving the organisation in line with the NHS Digital Joiners, Movers and Leavers Policy.
B21	Users shall comply with the NHS Digital Clear Desk policy.
B22	Users shall comply with requirements to wear ID at all times whilst working within the NHS Digital estate or premises.
B23	Users shall be vigilant and raise a concern if it is believed that someone is misusing NHS Digital's information or electronic equipment.
B24	Users shall be responsible for their own actions and act responsibly and professionally, following the NHS Digital's Business Code of Conduct.
B25	Never undertake illegal activity, or any activity that would be harmful to NHS Digital's reputation or jeopardise staff/citizen data, or NHS Digital's technology.
B26	Users shall not undertake any form of gaming, lottery or betting using NHS Digital equipment.
B27	Users shall not trade or canvass support for any organisation on official premises, whether it is for personal gain from any type of transaction or on behalf of external bodies.
B28	Users shall not send messages or material that solicit or promote religious, political or otherwise business-related causes, unless authorised by NHS Digital.
B29	Users shall not provide unauthorised views or commitments that could appear to be on behalf of NHS Digital.
B30	Users shall not login to any NHS Digital systems using another user's credentials.
B31	Users shall not download music, video or other media files for non-business purposes, or store such files on network drives.
B32	Users shall not attempt to compromise or gain unauthorised access to NHS Digital IT, telephony or content, or prevent legitimate access to it.
B33	Users shall not access personal webmail accounts on NHS Digital equipment.
B34	Users shall be responsible for keeping all assets assigned to them safe and secure, and immediately report any loss or damage of equipment to their line manager and the National Service Desk.
B35	Users should be careful not to be overheard or over-shouldered in public areas when conducting NHS Digital business.
B36	Users shall protect NHS Digital equipment appropriately outside of NHS Digital buildings e.g. laptops should always be powered off and protected in a case/bag.
B37	Users shall not have network access smart cards and/or lock the screen when leaving temporarily devices that are in use.
B38	Users shall not actively seek to undermine or circumvent any physical security controls such as barriers, doors or secure cupboards.
B39	Users should be wary of leaving assets in plain sight in parked vehicles and consider carrying them or securing them in the boot.
B40	Users shall not use any type of applications and/or devices to circumvent management or security controls.

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

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

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

2. Supplier must always be prepared for contract exit

- 2.1 If requested by the Buyer, the Supplier shall within 30 days provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value, as is relevant to the work package/s being provided.
- 2.2 During the Contract Period, if requested by the Buyer and as is relevant to the work package/s being provided, the Supplier shall promptly:
- 2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and
- 2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables.

("Registers").

- 2.3 The Supplier shall:

- 2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and
 - 2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.
- 2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

3. Assisting re-competition for Deliverables

- 3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "Exit Information").
- 3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
- 3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).
- 3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

- 4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.
- 4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within

twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

- 4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;
- 4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;
- 4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;
- 4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;
- 4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;
- 4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;
- 4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;
- 4.3.8 proposals for the disposal of any redundant Deliverables and materials;
- 4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and
- 4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

- 4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:
 - (a) every six (6) months throughout the Contract Period; and
 - (b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;
 - (c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

- (d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

- 4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
- 4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

- 5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:
 - 5.1.1 the nature of the Termination Assistance required; and
 - 5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.
- 5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:
 - 5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and
 - 5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.
- 5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than twenty (20) Working Days' written notice upon the Supplier.
- 5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

- 6.1 Throughout the Termination Assistance Period the Supplier shall:
- 6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;
 - 6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
 - 6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
 - 6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
 - 6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
 - 6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
- 6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.
- 6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

- 7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.
- 7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
- 7.2.1 vacate any Buyer Premises;
 - 7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for

making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

- (a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and
- (b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

- 8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or
- 8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

- (a) the Exclusive Assets that are not Transferable Assets; and
- (b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

- 8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**),

in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

- 8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.
- 8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
- 8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
- 8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
- 8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
- 8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
- 8.7 The Buyer shall:
- 8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
- 8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 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 Supplier's Contract Manager's responsibilities and obligations;
 - 3.1.3 able to cancel any delegation and recommence the position himself; and
 - 3.1.4 replaced only after the Buyer has received notification of the proposed change.
- 3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager(s) in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

- 3.3 Receipt of communication from the Supplier's Contract Manager(s) by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

- 4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
- 5.2.1 the identification and management of risks;
 - 5.2.2 the identification and management of issues; and
 - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer and the Supplier have identified.

Call-Off Schedule 20 (Call-Off Specification)

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

The Deliverables are to be agreed at individual work package/project level, however the future Services and Deliverables will be aligned to Lot 3 Complex and Transformation, as set out below:

Business;

- Change management;
- Complex programmes;
- Digital, technology and cyber services;
- Finance;
- HR;
- Organisation and operating model;
- Performance transformation;
- Procurement and/or supply chain;
- Project and programme management;
- Strategy and/or policy;
- Supplier side services and delivery;
- Transformation management.

The Parties acknowledge that these requirements are not fully defined at the point of awarding this Call-Off Contract and will be developed over the term of this Call-Off Contract as several projects ("Future Services"). Future Services will be called off using the Commissioning Process outlined at Appendix 1 to this Call-Off Order Form.

The Buyer is not obliged to request any Future Services. In the event that the Buyer does raise a request for Future Services, the Supplier is required to respond in accordance with the Commissioning Process outlined in Appendix 1 to this Order Form and the Call-Off Contract.