

Contract for the provision of bill validation and cost recovery services for Educational Institutions across England

Contract ref. – Con_25837

Order Form

CALL-OFF REFERENCE:	con_25837
THE BUYER:	SECRETARY OF STATE FOR EDUCATION
BUYER ADDRESS	Department for Education, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
THE SUPPLIER:	PROFESSIONAL COST MANAGEMENT GROUP LIMITED
SUPPLIER ADDRESS:	Calder House, St Georges Park Kirkham Lancashire PR4 2DZ
REGISTRATION NUMBER:	6511368
DUNS NUMBER:	211094588
SID4GOV ID:	n/a

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated Aug 22, 2024.

It's issued under the Framework Contract with the reference number RM6226 for the provision of Debt Resolution Services.

CALL-OFF LOT(S):

Lot 17: Spend Analytics and Recovery Services (Utilities Spend Recovery Review)

CALL-OFF INCORPORATED TERMS:

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

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. [Joint Schedule 1](#) (Definitions and Interpretation) of RM6226
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
 - Joint Schedules for RM6226
 - [Joint Schedule 2](#) (Variation Form and Change Control Procedure)
 - [Joint Schedule 3](#) (Insurance Requirements)
 - [Joint Schedule 4](#) (Commercially Sensitive Information)
 - [Joint Schedule 6](#) (Key Subcontractors)
 - [Joint Schedule 10](#) (Rectification Plan)
 - [Joint Schedule 11](#) (Processing Data)
 - Call-Off Schedules for RM6226
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 2 (Staff Transfer)
 - Call-Off Schedule 3 (Continuous Improvement)
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedule 7 (Key Supplier Staff)
 - Call-Off Schedule 9 (Security Requirements)
 - Call-Off Schedule 10 (Exit Management)
 - Call-Off Schedule 12 (Clustering)
 - Call-Off Schedule 13 (Implementation Plan)
 - Call-Off Schedule 14 (Service Levels)
 - Call-Off Schedule 15 (Call-Off Contract Management)
 - Call-Off Schedule 20 (Call-Off Specification))
5. [CCS Core Terms](#) (version 3.0.11)
6. [Joint Schedule 5](#) (Corporate Social Responsibility) RM6226
7. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

CALL-OFF SPECIAL TERMS:

The following Special Terms are incorporated into this Call-Off Contract:

None

CALL-OFF START DATE:

27 August 2024

CALL-OFF EXPIRY DATE:

31 May 2026

CALL-OFF INITIAL PERIOD:

21 Months

CALL-OFF OPTIONAL EXTENSION PERIOD:

12 Months

CALL-OFF DELIVERABLES:

See details in Call-Off Schedule 20 (Call-Off Specification)

MAXIMUM LIABILITY:

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £500,000

CALL-OFF CHARGES:

See details in Call-Off Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES:

None

PAYMENT METHOD:

BACS transfer, unless otherwise stated in individual Engagement Letters signed by the School.

BUYER'S INVOICE ADDRESS:

As stated in individual Engagement Letters signed by the School.

BUYER'S AUTHORISED REPRESENTATIVE:

[REDACTED]

BUYER'S ENVIRONMENTAL POLICY:

available online at: <https://www.gov.uk/government/publications/sustainability-and-climate-change-strategy/sustainability-and-climate-change-a-strategy-for-the-education-and-childrens-services-systems>

BUYER'S SECURITY POLICY:

Appended at Call-Off Schedule 9

SUPPLIER'S AUTHORISED REPRESENTATIVE:

[REDACTED]

SUPPLIER'S CONTRACT MANAGER:

[REDACTED]

PROGRESS REPORT FREQUENCY:

DfE quarterly reports. Progress reported to schools as per their instruction

PROGRESS MEETING FREQUENCY:

Quarterly during the first week of each quarter.

KEY STAFF:

[REDACTED]

KEY SUBCONTRACTOR(S):

n/a

COMMERCIALLY SENSITIVE INFORMATION:

Not applicable

SERVICE CREDITS:

Not applicable

ADDITIONAL INSURANCES:

Not applicable

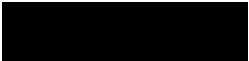
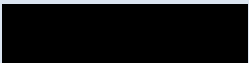

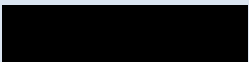
GUARANTEE:


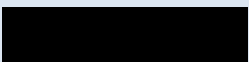

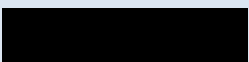
Not applicable

SOCIAL VALUE COMMITMENT:

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

SIGNATURES:

For and on behalf of the Supplier:	
Signature:	
Name:	
Role:	
Date:	

For and on behalf of the Buyer:	
Signature:	
Name:	
Role:	
Date:	

Contents

Call-Off Schedule 1 (Transparency Reports)	8
Annex A: List of Transparency Reports	9
Call-Off Schedule 2 (Staff Transfer).....	10
Call-Off Schedule 3 (Continuous Improvement)	26
Call-Off Schedule 4 (Call Off Tender)	28
Call-Off Schedule 5 (Pricing Details).....	29
Call-Off Schedule 7 (Key Supplier Staff)	30
Call-Off Schedule 9 (Security Requirements).....	32
Appendix 1	58
Call-Off Schedule 10 (Exit Management).....	59
Call-Off Schedule 12 (Clustering)	67
Annex A – Cluster Members	1
Call-Off Schedule 13 (Implementation Plan and Testing).....	1
Call-Off Schedule 14 (Service Levels)	5
Part A: Service Levels and Service Credits	6
Call-Off Schedule 15 (Call-Off Contract Management).....	9
Call-Off Schedule 20 (Call-Off Specification).....	11
Annex 1 to Joint Schedule 11 - Processing Personal Data	15

Call-Off Schedule 1 (Transparency Reports)

- 1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (<https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles>)). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.
- 1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.
- 1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.
- 1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance	Details of activities under the call-off agreement including data specified in Call-off schedule 20.	MS Excel	Quarterly
Call-Off Contract Charges	Summary of costs recovered and charges invoiced per activity	MS Excel	Quarterly

Call-Off Schedule 2 (Staff Transfer)

1. Definitions

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

<p>"Acquired Rights Directive"</p>	<p>1 the European Council Directive 77/187/EEC on the approximation of laws of European member states relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, as amended or re-enacted from time to time;</p> <p>2</p>
<p>"Employee Liability"</p>	<p>3 all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:</p> <ul style="list-style-type: none"> a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments; b) unfair, wrongful or constructive dismissal compensation; c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay; d) compensation for less favourable treatment of part-time workers or fixed term employees; e) outstanding employment debts and unlawful deduction of wages including any PAYE and National Insurance Contributions;

	<p>f) employment claims whether in tort, contract or statute or otherwise;</p> <p>g) any investigation relating to employment matters by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;</p>
"Former Supplier"	a supplier supplying services to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Services (or any part of the Services) and shall include any Subcontractor of such supplier (or any Subcontractor of any such Subcontractor);
"New Fair Deal"	<p>the revised Fair Deal position set out in the HM Treasury guidance: <i>"Fair Deal for Staff Pensions: Staff Transfer from Central Government"</i> issued in October 2013 including:</p> <ul style="list-style-type: none"> (i) any amendments to that document immediately prior to the Relevant Transfer Date; and (ii) any similar pension protection in accordance with the Annexes D1-D3 inclusive to Part D of this Schedule as notified to the Supplier by the Buyer;
"Old Fair Deal"	HM Treasury Guidance <i>"Staff Transfers from Central Government: A Fair Deal for Staff Pensions"</i> issued in June 1999 including the supplementary guidance <i>"Fair Deal for Staff pensions: Procurement of Bulk Transfer Agreements and Related Issues"</i> issued in June 2004;
"Partial Termination"	the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);
"Relevant Transfer"	a transfer of employment to which the Employment Regulations applies;
"Relevant Transfer Date"	in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place. For the purposes of Part D: Pensions and its Annexes, where the Supplier or a Subcontractor was the Former Supplier and there is no Relevant Transfer of the Fair Deal Employees because they remain continuously employed by the Supplier (or

	Subcontractor), references to the Relevant Transfer Date shall become references to the Start Date;
"Staffing Information"	<p>in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Legislation), but including in an anonymised format:</p> <ul style="list-style-type: none"> (a) their ages, dates of commencement of employment or engagement, gender and place of work; (b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise; (c) the identity of the employer or relevant contracting Party; (d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments; (e) their wages, salaries, bonuses and profit sharing arrangements as applicable; (f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them; (g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims); (h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence; <p>(i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and</p>

	(j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;
"Supplier's Final Supplier Personnel List"	a list provided by the Supplier of all Supplier Staff whose will transfer under the Employment Regulations on the Service Transfer Date;
"Supplier's Provisional Supplier Personnel List"	a list prepared and updated by the Supplier of all Supplier Staff who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;
"Term"	the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract;
"Transferring Buyer Employees"	those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date;
"Transferring Former Supplier Employees"	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date.

2. INTERPRETATION

- 2.1 Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Subcontractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Subcontractor, as the case may be and where the Subcontractor fails to satisfy any claims under such indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.
- 2.2 The provisions of Paragraphs 2.1 and 2.6 of Part A, Paragraph 3.1 of Part B, Paragraphs 1.5, 1.7 and 1.9 of Part C, Part D and Paragraphs 1.4, 2.3 and 2.8 of Part E of this Schedule (together "Third Party Provisions") confer benefits on third parties (each such person a "Third Party Beneficiary") and are intended to be enforceable by Third Party Beneficiaries by virtue of the CRTPA.
- 2.3 Subject to Paragraph 2.2 above, a person who is not a Party to this Call-Off Contract has no right under the CRTPA to enforce any term of this Call-Off Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.
- 2.4 No Third Party Beneficiary may enforce, or take any step to enforce, any Third Party Provision without the prior written consent of the Buyer, which may, if given, be given on and subject to such terms as the Buyer may determine.

- 2.5 Any amendments or modifications to this Call-Off Contract may be made, and any rights created under Paragraph 2.2 above may be altered or extinguished, by the Parties without the consent of any Third Party Beneficiary.

3. Which parts of this Schedule apply

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

- Part C (No Staff Transfer on the Start Date)
- Part E (Staff Transfer on Exit)

Part C: No Staff Transfer on the Start Date

1. What happens if there is a staff transfer

- 1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.
- 1.2 If any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive then:
- 1.2.1 the Supplier shall, and shall procure that the relevant Subcontractor shall, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing and, where required by the Buyer, notify the Former Supplier in writing; and
 - 1.2.2 the Buyer and/or the Former Supplier may offer (or may procure that a third party may offer) employment to such person within 15 Working Days of the notification from the Supplier or the Subcontractor (as appropriate) or take such other reasonable steps as the Buyer or Former Supplier (as the case may be) it considers appropriate to deal with the matter provided always that such steps are in compliance with applicable Law.
- 1.3 If an offer referred to in Paragraph 1.2.2 is accepted (or if the situation has otherwise been resolved by the Buyer and/or the Former Supplier),, the Supplier shall, or shall procure that the Subcontractor shall, immediately release the person from his/her employment or alleged employment.
- 1.4 If by the end of the 15 Working Day period referred to in Paragraph 1.2.2:
- 1.4.1 no such offer of employment has been made;
 - 1.4.2 such offer has been made but not accepted; or

1.4.3 the situation has not otherwise been resolved;

the Supplier may within 5 Working Days give notice to terminate the employment or alleged employment of such person.

1.5 Subject to the Supplier and/or the relevant Subcontractor acting in accordance with the provisions of Paragraphs 1.2 to 1.4 and in accordance with all applicable employment procedures set out in applicable Law and subject also to Paragraph 1.8 the Buyer shall:

1.5.1 indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier takes, or shall procure that the Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities; and

1.5.2 procure that the Former Supplier indemnifies the Supplier and/or any Subcontractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2 made pursuant to the provisions of Paragraph 1.4 provided that the Supplier takes, or shall procure that the relevant Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.

1.6 If any such person as is described in Paragraph 1.2 is neither re employed by the Buyer and/or the Former Supplier as appropriate nor dismissed by the Supplier and/or any Subcontractor within the 15 Working Day period referred to in Paragraph 1.4 such person shall be treated as having transferred to the Supplier and/or the Subcontractor (as appropriate) and the Supplier shall, or shall procure that the Subcontractor shall, comply with such obligations as may be imposed upon it under Law.

1.7 Where any person remains employed by the Supplier and/or any Subcontractor pursuant to Paragraph 1.6, all Employee Liabilities in relation to such employee shall remain with the Supplier and/or the Subcontractor and the Supplier shall indemnify the Buyer and any Former Supplier, and shall procure that the Subcontractor shall indemnify the Buyer and any Former Supplier, against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.

1.8 The indemnities in Paragraph 1.5:

1.8.1 shall not apply to:

(a) any claim for:

(i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or

- (ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

in any case in relation to any alleged act or omission of the Supplier and/or Subcontractor; or

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

1.8.2 shall apply only where the notification referred to in Paragraph 1.2.1 is made by the Supplier and/or any Subcontractor to the Buyer and, if applicable, Former Supplier within 6 months of the Start Date.

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

2. Limits on the Former Supplier's obligations

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

Part E: Staff Transfer on Exit

1. Obligations before a Staff Transfer

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

- 1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;
- 1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;
- 1.1.3 the date which is 12 Months before the end of the Term; and
- 1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

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

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

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

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

1.5 From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not, and agrees to procure that each Subcontractor shall not, assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall not without the approval of the Buyer (not to be unreasonably withheld or delayed):

:

- 1.5.1 replace or re-deploy any Supplier Staff listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person he/she replaces

- 1.5.2 make, promise, propose, permit or implement any material changes to the terms and conditions of employment of the Supplier Staff (including pensions and any payments connected with the termination of employment);
- 1.5.3 increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Staff save for fulfilling assignments and projects previously scheduled and agreed;
- 1.5.4 introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;
- 1.5.5 increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);
- 1.5.6 terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;

and shall promptly notify, and procure that each Subcontractor shall promptly notify, the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Subcontractor of any notice to terminate employment given by the Supplier or relevant Subcontractor or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect.

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

- 1.6.1 the numbers of employees engaged in providing the Services;
- 1.6.2 the percentage of time spent by each employee engaged in providing the Services;
- 1.6.3 the extent to which each employee qualifies for membership of any of the Statutory Schemes or any Broadly Comparable scheme set up pursuant to the provisions of any of the Annexes to Part D (Pensions) (as appropriate); and
- 1.6.4 a description of the nature of the work undertaken by each employee by location.

- 1.7 The Supplier shall provide, and shall procure that each Subcontractor shall provide, all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Subcontractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient

information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide, and shall procure that each Subcontractor shall provide, to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Subcontractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:

- 1.7.1 the most recent month's copy pay slip data;
- 1.7.2 details of cumulative pay for tax and pension purposes;
- 1.7.3 details of cumulative tax paid;
- 1.7.4 tax code;
- 1.7.5 details of any voluntary deductions from pay; and
- 1.7.6 bank/building society account details for payroll purposes.

2. Staff Transfer when the contract ends

- 2.1 The Buyer and the Supplier acknowledge that subsequent to the commencement of the provision of the Services, the identity of the provider of the Services (or any part of the Services) may change (whether as a result of termination or Partial Termination of the relevant Contract or otherwise) resulting in the Services being undertaken by a Replacement Supplier and/or a Replacement Subcontractor. Such change in the identity of the supplier of such services may constitute a Relevant Transfer to which the Employment Regulations and/or the Acquired Rights Directive will apply. The Buyer and the Supplier agree that, as a result of the operation of the Employment Regulations, where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Subcontractor (as the case may be) and each such Transferring Supplier Employee.
- 2.2 The Supplier shall, and shall procure that each Subcontractor shall, comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date and shall perform and discharge, and procure that each Subcontractor shall perform and discharge, all its obligations in respect of all the Transferring Supplier Employees arising in respect of the period up to (and including) the Service Transfer Date (including (without limit) the payment of all remuneration, benefits, entitlements, and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Schemes which in any case are attributable in whole or in part to the period ending on (and including) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between: (i) the

Supplier and/or the Subcontractor (as appropriate); and (ii) the Replacement Supplier and/or Replacement Subcontractor.

2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor against any Employee Liabilities arising from or as a result of:

- 2.3.1 any act or omission of the Supplier or any Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date;
- 2.3.2 the breach or non-observance by the Supplier or any Subcontractor occurring on or before the Service Transfer Date of:
 - (a) any collective agreement applicable to the Transferring Supplier Employees; and/or
 - (b) any other custom or practice with a trade union or staff association in respect of any Transferring Supplier Employees which the Supplier or any Subcontractor is contractually bound to honour;
- 2.3.3 any claim by any trade union or other body or person representing any Transferring Supplier Employees arising from or connected with any failure by the Supplier or a Subcontractor to comply with any legal obligation to such trade union, body or person arising on or before the Service Transfer Date;
- 2.3.4 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (a) in relation to any Transferring Supplier Employee, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on and before the Service Transfer Date; and
 - (b) in relation to any employee who is not identified in the Supplier's Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Supplier to the Buyer and/or Replacement Supplier and/or any Replacement Subcontractor, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising on or before the Service Transfer Date;
- 2.3.5 a failure of the Supplier or any Subcontractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees in respect of the period up to (and including) the Service Transfer Date);

- 2.3.6 any claim made by or in respect of any person employed or formerly employed by the Supplier or any Subcontractor other than a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List for whom it is alleged the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor may be liable by virtue of the relevant Contract and/or the Employment Regulations and/or the Acquired Rights Directive; and
 - 2.3.7 any claim made by or in respect of a Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee relating to any act or omission of the Supplier or any Subcontractor in relation to its obligations under regulation 13 of the Employment Regulations, except to the extent that the liability arises from the failure by the Buyer and/or Replacement Supplier to comply with regulation 13(4) of the Employment Regulations.
- 2.4 The indemnities in Paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Subcontractor whether occurring or having its origin before, on or after the Service Transfer Date including any Employee Liabilities:
 - 2.4.1 arising out of the resignation of any Transferring Supplier Employee before the Service Transfer Date on account of substantial detrimental changes to his/her working conditions proposed by the Replacement Supplier and/or any Replacement Subcontractor to occur in the period on or after the Service Transfer Date); or
 - 2.4.2 arising from the Replacement Supplier's failure, and/or Replacement Subcontractor's failure, to comply with its obligations under the Employment Regulations.
- 2.5 If any person who is not identified in the Supplier's Final Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Subcontractor pursuant to the Employment Regulations or the Acquired Rights Directive, then:
 - 2.5.1 the Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing; and
 - 2.5.2 the Supplier may offer (or may procure that a Subcontractor may offer) employment to such person, or take such other reasonable steps as it considered appropriate to deal the matter provided always that such steps are in compliance with Law, within 15 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Subcontractor.

- 2.6 If such offer of is accepted, or if the situation has otherwise been resolved by the Supplier or a Subcontractor, Buyer shall procure that the Replacement Supplier shall, or procure that the and/or Replacement Subcontractor shall, immediately release or procure the release the person from his/her employment or alleged employment;
- 2.7 If after the 15 Working Day period specified in Paragraph 2.5.2 has elapsed:
- 2.7.1 no such offer has been made:
 - 2.7.2 such offer has been made but not accepted; or
 - 2.7.3 the situation has not otherwise been resolved

the Buyer shall advise the Replacement Supplier and/or Replacement Subcontractor (as appropriate) that it may within 5 Working Days give notice to terminate the employment or alleged employment of such person;

- 2.8 Subject to the Replacement Supplier's and/or Replacement Subcontractor acting in accordance with the provisions of Paragraphs 2.5 to 2.7 and in accordance with all applicable proper employment procedures set out in applicable Law and subject to Paragraph 2.9 below, the Supplier will indemnify the Replacement Supplier and/or Replacement Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees pursuant to the provisions of Paragraph 2.7 provided that the Replacement Supplier takes, or shall procure that the Replacement Subcontractor takes, all reasonable steps to minimise any such Employee Liabilities.

- 2.9 The indemnity in Paragraph 2.8:

- 2.9.1 shall not apply to:

- (a) any claim for:

- (i) discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief; or
- (ii) equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees,

In any case in relation to any alleged act or omission of the Replacement Supplier and/or Replacement Subcontractor, or

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

- 2.9.2 shall apply only where the notification referred to in Paragraph 2.5.1 is made by the Replacement Supplier and/or Replacement

Subcontractor to the Supplier within 6 months of the Service Transfer Date..

- 2.10 If any such person as is described in Paragraph 2.5 is neither re-employed by the Supplier or any Subcontractor nor dismissed by the Replacement Supplier and/or Replacement Subcontractor within the time scales set out in Paragraphs 2.5 to 2.7, such person shall be treated as a Transferring Supplier Employee. .
- 2.11 The Supplier shall comply, and shall procure that each Subcontractor shall comply, with all its obligations under the Employment Regulations and shall perform and discharge, and shall procure that each Subcontractor shall perform and discharge, all its obligations in respect of any person identified in the Supplier's Final Supplier Personnel List before and on the Service Transfer Date (including the payment of all remuneration, benefits, entitlements and outgoings, all wages, accrued but untaken holiday pay, bonuses, commissions, payments of PAYE, national insurance contributions and pension contributions and such sums due as a result of any Fair Deal Employees' participation in the Schemes and any requirement to set up a broadly comparable pension scheme which in any case are attributable in whole or in part in respect of the period up to (and including) the Service Transfer Date) and any necessary apportionments in respect of any periodic payments shall be made between:
- (b) the Supplier and/or any Subcontractor; and
 - (c) the Replacement Supplier and/or the Replacement Subcontractor.
- 2.12 The Supplier shall, and shall procure that each Subcontractor shall, promptly provide the Buyer and any Replacement Supplier and/or Replacement Subcontractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor, shall promptly provide to the Supplier and each Subcontractor in writing such information as is necessary to enable the Supplier and each Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.
- 2.13 Subject to Paragraph 2.14, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Subcontractor and its Subcontractors against any Employee Liabilities arising from or as a result of:
- 2.13.1 any act or omission of the Replacement Supplier and/or Replacement Subcontractor in respect of any Transferring Supplier Employee in the Supplier's Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee;
 - 2.13.2 the breach or non-observance by the Replacement Supplier and/or Replacement Subcontractor on or after the Service Transfer Date of:

- (a) any collective agreement applicable to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List; and/or
 - (b) any custom or practice in respect of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List which the Replacement Supplier and/or Replacement Subcontractor is contractually bound to honour;
- 2.13.3 any claim by any trade union or other body or person representing any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List arising from or connected with any failure by the Replacement Supplier and/or Replacement Subcontractor to comply with any legal obligation to such trade union, body or person arising on or after the Service Transfer Date;
- 2.13.4 any proposal by the Replacement Supplier and/or Replacement Subcontractor to change the terms and conditions of employment or working conditions of any Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List on or after their transfer to the Replacement Supplier or Replacement Subcontractor (as the case may be) on the Service Transfer Date, or to change the terms and conditions of employment or working conditions of any person identified in the Supplier's Final Supplier Personnel List who would have been a Transferring Supplier Employee but for their resignation (or decision to treat their employment as terminated under regulation 4(9) of the Employment Regulations) before the Service Transfer Date as a result of or for a reason connected to such proposed changes;
- 2.13.5 any statement communicated to or action undertaken by the Replacement Supplier or Replacement Subcontractor to, or in respect of, any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List on or before the Service Transfer Date regarding the Relevant Transfer which has not been agreed in advance with the Supplier in writing;
- 2.13.6 any proceeding, claim or demand by HMRC or other statutory authority in respect of any financial obligation including, but not limited to, PAYE and primary and secondary national insurance contributions:
 - (a) in relation to any Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List, to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising after the Service Transfer Date; and

- (b) in relation to any employee who is not a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List, and in respect of whom it is later alleged or determined that the Employment Regulations applied so as to transfer his/her employment from the Supplier or Subcontractor, to the Replacement Supplier or Replacement Subcontractor to the extent that the proceeding, claim or demand by HMRC or other statutory authority relates to financial obligations arising after the Service Transfer Date;

2.13.7 a failure of the Replacement Supplier or Replacement Subcontractor to discharge or procure the discharge of all wages, salaries and all other benefits and all PAYE tax deductions and national insurance contributions relating to the Transferring Supplier Employees identified in the Supplier's Final Supplier Personnel List in respect of the period from (and including) the Service Transfer Date; and

2.13.8 any claim made by or in respect of a Transferring Supplier Employee identified in the Supplier's Final Supplier Personnel List or any appropriate employee representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee relating to any act or omission of the Replacement Supplier or Replacement Subcontractor in relation to obligations under regulation 13 of the Employment Regulations.

2.14 The indemnities in Paragraph 2.13 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Subcontractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Subcontractor (as applicable) to comply with its obligations under the Employment Regulations.

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

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

2. Supplier's Obligations

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

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

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

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

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

- 2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.
- 2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.
- 2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.
- 2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
- 2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and
 - 2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.
- 2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.
- 2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.
- 2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.
- 2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 4 (Call Off Tender)



Call-Off Schedule 5 (Pricing Details)

Banding	1) Collections >£1 <£50k	2)Collections >£50k <£150k	3)Collections >£150k <£500k	4)Collections >£500k
Commission Price %				

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 9 (Security Requirements)

1. Definitions

In this Schedule, the following definitions shall apply and be supplemental to those in Joint Schedule 1 (Definitions):

"Accreditation"	the assessment of the Core Information Management System in accordance with Part C of this Schedule by the Buyer or an independent information risk manager/professional appointed by the Buyer, which results in an Accreditation Decision;
"Accreditation Decision"	is the decision of the Buyer, taken in accordance with the process set out in Paragraph 4 of Part C of this Schedule, to issue the Supplier with a Risk Management Approval Statement or a Risk Management Rejection Notice in respect of the Core Information Management System;
"Accreditation Plan"	the Supplier's plan to attain an Accreditation Approval Statement from the Buyer, which is prepared by the Supplier and Approved by the Buyer in accordance with Part C of this Schedule;
"Anti-Malicious Software"	Software that scans for and identifies possible Malicious Software in the ICT Environment;
"Breach of Security"	<p>the occurrence of:</p> <ul style="list-style-type: none"> (a) any unauthorised access to or use of the Services, the Sites, the Supplier System, and/or any information or data (including the Confidential Information and the Government Data) used by the Buyer, the Supplier or any Subcontractor in connection with this Call-Off Contract; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including copies of such information or data, used by the Buyer, the Supplier and/or any Subcontractor in connection with this Call-Off Contract; and/or (c) any part of the Supplier System ceasing to be compliant with the Certification Requirements, <p>in each case as more particularly set out in the Security Requirements in Framework Schedule 1 (Specification) and the Order Form and the Security Requirements;</p>

"Certification Requirements"	the requirements set out in Part E of this Schedule;
"CHECK Service Provider"	a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC Services required by the Paragraph 4.2 of Part C of this Schedule;
"CIMS Subcontractor"	a Subcontractor that provides or operates the whole, or a substantial part, of the Core Information Management System;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources) which the Buyer has determined in accordance with the Security Requirements;
General Security Requirements	the Security Requirements that shall apply to any Supplier and / or Subcontractor that processes Personal Data;
"Higher Risk Subcontractor"	<p>a Subcontractor that Processes Government Data, where that data includes either:</p> <p>(a) the Personal Data of 1000 or more individuals in aggregate during the period between the Call-Off Start Date and the End Date; or</p> <p>(b) Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;</p>
"IT Health Check" (ITHC)	has the meaning given Paragraph 4.2 of Part C of this Schedule;
Incident Management Process	is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services and which shall be prepared by the Supplier in accordance with Paragraph 13.2 of Part A of this Schedule and as set out by the Supplier and Approved by the Buyer within the template set out in Section 23 of Appendix 1 of this Schedule;
"Information Assurance Assessment"	is the set of policies, procedures, systems and processes which the Supplier shall implement,

	maintain and update in accordance with Part B of this Schedule in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Appendix 1 of this Schedule;
"Information Management System"	the Core Information Management System and the Wider Information Management System;
"Information Security Approval Statement"	a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Buyer: (i) is satisfied that the identified risks have been adequately and appropriately addressed; (ii) the Buyer has accepted the residual risks; and (iii) the Supplier may use the Information Management System to Process Government Data;
"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;
"Medium Risk Subcontractor"	<p>a Subcontractor that Processes Government Data, where that data</p> <p>(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Call-Off Start Date and the End Date; and</p> <p>(b) does not include Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned;</p>
"Required Changes Register"	<p>is a register which forms part of the Risk Management Documentation which records each of the changes that the Supplier has agreed with the Buyer to be made to the Core Information System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in the following Paragraphs within:</p> <ul style="list-style-type: none"> ● 1.3 of Part B; ● 4 of Part C; ● 3 of Part D;

	together with the date on which each change shall be implemented and the date on which each change was implemented;
"Risk Management Approval Statement"	a notice issued by the Buyer which sets out the information risks associated with using the Core Information Management System and confirms that the Buyer is satisfied that the identified risks have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer;
"Risk Management Documentation"	is the information and supporting documentation that the Supplier develops and provides to the Buyer when completing section 11 of the Security Management Plan;
"Risk Management Reject Notice"	has the meaning given in Paragraph 4.8.2;
"Security Management Plan"	comprises all information required from the Supplier in order to demonstrate compliance with the Security Requirements that must be presented in the templates set out in Appendix 1;
Security Requirements	the security requirements that the Supplier and each Subcontractor must comply with during the Contract Period as set out in the this Schedule;
"Security Test"	has the meaning given Paragraphs 4 in Part C and Part D of this Schedule;
Security Working Group	the meeting led by the Buyer (or their agent) with the Supplier to discuss the Security Management Plan and any risks, issues and controls the Supplier has put into place to ensure they are delivering the Security Requirements. The timing, required attendees and periodicity of the meetings will be defined by the Buyer during implementation, but should be no less than quarterly and should include the Supplier's Staff with the relevant expertise;
"Special Category of Personal Data"	the categories of Personal Data set out in Article 9(1) of GDPR;
"Statement of Information Risk Appetite"	the document that sets-out the type and level of risk that the Buyer is prepared to accept;
"Subcontractor Security Requirements"	any Security Requirements that must be delivered by Subcontractors;
"Vulnerability Correction Plan"	has the meaning given in Paragraph Part C Paragraph 4.3.3.1 of this Schedule;
"Wider Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Subcontractors to Process Government Data which

	have not been determined by the Buyer to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources).
--	---

2. **Part A Introduction**

2.1. This Schedule sets out:

- 2.1.1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of Government Data, the Services and the Information Management System;
- 2.1.2. the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;
- 2.1.3. the Security Requirements with which the Supplier must comply, which are dependent upon the applicable Lot(s) awarded to the Supplier under the Framework Contract;
- 2.1.4. the tests which the Supplier shall conduct on the Information Management System during the Term;
- 2.1.5. the Supplier's obligations to:
 - 2.1.5.1. return or destroy Government Data on the expiry or earlier termination of this Call-Off Contract; and
 - 2.1.5.2. prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 8; and
 - 2.1.5.3. report Breaches of Security to the Buyer.
- 2.1.6. the applicable Tier of Security Requirements required to be complied with by the Supplier are summarised in Table 1 below:

Table 1:

Tier	Lot	Summary Security Requirements	Certification Requirements
1.	1	<u>General Security Requirements (Part B) plus PSC Accreditation (Part C)</u> The Supplier is also required to: <ul style="list-style-type: none"> a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the 	ISO 27001:2017 and Cyber Essentials (CE) + and PCI-DSS

		Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request .	
2.	5, 6, 7, 20	<u>General Security Requirements (Part A) plus PSC Assurance (Part D) for Lot 20</u> The Supplier is also required to: a) ensure that terms and conditions no less onerous than those outlined in Part D of this Schedule are also flowed down within it's Subcontracts with Subcontractors; b) ensure that it's Subcontractors comply with the Security Requirements; and c) provide all documentation relating to the Subcontractors delivery of the Security Requirements including the Subcontractors Security Management Plans, to the Buyer immediately upon written request.	ISO 27001:2017 and CE+ and PCI-DSS
3.	2, 3, 8, 9, 10, 11, 12, 13, 14	<u>General Security Requirements (Part B)</u>	ISO 27001:2017 and CE+
4.	4, 15, 16, 17, 18, 19	<u>General Security Requirements (Part B) when handling Personal Data, otherwise N/A</u>	CE

3. Principles of Security

3.1. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently on the security of:

- 3.1.1. the Sites;
- 3.1.2. the Supplier System;
- 3.1.3. the Information Management System, Core information Management System and Wider Information Management System, as applicable; and
- 3.1.4. the Services.

3.2. Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Government Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:

- 3.2.1. the security, confidentiality, integrity and availability of the Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; and
- 3.2.2. the security of the Information Management System.

- 3.3. The Supplier shall:
 - 3.3.1. comply with the Security Requirements in this Schedule; and
 - 3.3.2. ensure that each Subcontractor that Processes Government Data complies with the Subcontractor Security Requirements in this Schedule.
- 3.4. The Supplier shall provide the Buyer with access to Supplier Staff responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Schedule at reasonable times on reasonable notice.
- 3.5. The Buyer may at its sole discretion appoint an agent to act on its behalf with regards to its engagement with the Supplier regarding the Security Requirements.

Part B General Security Requirements

1. The Security Management Plan

- 1.1 The Security Management Plan includes details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement.
- 1.2 The Supplier shall complete the Security Management Plan Template (Appendix 1) detailing how they will deliver the Security Requirements and the necessary information required for the applicable Tier(s) for the Lot(s) awarded to the Supplier. Any element that does not apply or only partially applies should be explained within the Template. If a Supplier is delivering Services in respect of more than 1 Lot, it must complete a separate Security Risk Management Template for each Lot.
- 1.3 Where there has been a Variation or Change to the Services which affects any aspect of the Security Requirements, CCS and the relevant Buyers must be notified immediately in writing of this fact and the extent of its effect or believed effect on the Security Requirements and / or the Tier of the Security Requirements that the Supplier should apply to the Service (actual or potential).
- 1.4 The Supplier shall complete the Security Management Plan to demonstrate and document how they comply with the Security Requirements. A draft Security Management Plan shall be made available to the Buyer prior to the Call-Off Contract Effective Date unless already Approved by the Buyer.
- 1.5 The Security Management Plan should be provided to the Buyer in accordance with the Buyer's requirements and as set out within the Implementation Plan, but in any case, unless already Approved by the Buyer, this should be prior to the Service Effective Date.

2. Security Classification of Information

- 2.1 If the provision of the Services requires the Supplier to Process Government Data which is classified as: OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

3. End User Devices

- 3.1 The Supplier shall ensure that any Government Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has

been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement.

- 3.2 The Supplier shall ensure that any device which is used to Process Government Data meets all of the Security Requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>

- 3.3 The Supplier must ensure that their EUD's require all Supplier Staff to authenticate themselves before gaining access to the device. All the Supplier's EUD's must encrypt all data at rest using a reputable full disk encryption solution that has been formally assured through a recognised certification process agreed with the Buyer, except where the Buyer has already Approved a suitable alternative arrangement. The Supplier's EUD's must be configured to automatically lock the screen after a period of inactivity and this must be agreed with the Buyer in writing.

4. **Location of Government Data**

- 4.1 The Supplier shall not and shall procure that none of its Subcontractors Process Government Data outside the UK without the Approval of the Buyer, which may be subject to conditions and that it shall comply with Joint Schedule 11 (Processing Data).

5. **Vulnerabilities and Corrective Action**

- 5.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.

- 5.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability.

- 5.3 The Supplier shall utilise scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

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

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

- 5.4 Subject to Paragraph 5.5, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

- 5.4.1 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

- 5.4.2 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

- 5.4.3 60 days after the public release of patches for those vulnerabilities categorised as 'Other'.

- 5.5 The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 5.4 shall be extended where:

- 5.5.1 the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by

the Supplier within the timescales set out in Paragraph 5.4 if the vulnerability becomes exploitable within the context of the Services;

- 5.5.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer;
- 5.5.3 the Buyer Approves to a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan; or
- 5.5.4 the Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Contract Period, unless otherwise Approved by the Buyer. All COTS Software should be no more than N-1 versions behind the latest software release.

6. Networking

- 6.1 The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted using TLS version 1.2 as a minimum.

7. Personnel Security

- 7.1 All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.
- 7.2 The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Staff who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which is classified as OFFICIAL-SENSITIVE.
- 7.3 The Supplier shall not permit Supplier Staff who fail the security checks required by Paragraphs 7.1 and 7.2 to be involved in the management and/or provision of the Services except where the Buyer

Approves the involvement of the named individual in the management and/or provision of the Services.

7.4 The Supplier shall ensure that Supplier Staff are only granted such access to Government Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.

7.5 The Supplier shall ensure that Supplier Staff who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its Subcontractors), have their rights to access the Government Data revoked within 1 Working Day

8. Identity, Authentication and Access Control

8.1 The Supplier shall operate an access control regime to ensure:

8.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

8.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.

8.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require to perform the Services under the Contract.

8.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such records available to the Buyer on request.

9. Audit and Protective Monitoring

9.1 The Supplier shall collect audit records which relate to security events in the Core Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Core Information Management System, to enable the identification of (without limitation) changing access

trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Government Data.

9.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

9.3 The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

10. **Secure Architecture**

10.1 The Supplier shall design the Core Information Management System in accordance with:

10.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;

10.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main> ; and

10.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

11. **Malicious Software**

11.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Government Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

11.2 If Malicious Software is found, the Parties shall cooperate 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 Services to their desired operating efficiency.

11.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 11.1 shall be borne by the Parties as follows:

11.3.1 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 the Data

was provided to the Supplier, unless the Buyer had instructed the Supplier to quarantine and check the data for Malicious Software and the Supplier had failed to do so, and

11.3.2 by the Buyer, in any other circumstance.

12. Data Destruction or Deletion

12.1 The Supplier shall:

- 12.1.1 prior to securely sanitising any Government Data or when requested the Supplier shall provide the Buyer with two copies of all Buyer Data in an agreed open format;
- 12.1.2 have documented processes to ensure the availability of Government Data in the event of the Supplier ceasing to trade;
- 12.1.3 securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;
- 12.1.4 securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific requirements in this Call-Off Contract and, in the absence of any such requirements, as agreed by the Buyer in writing; and
- 12.1.5 implement processes which address the CPNI and NCSC guidance on secure sanitisation.

13. Breach of Security

13.1 If either Party becomes aware or reasonably suspects of a Breach of Security it shall notify the other in accordance with the Incident Management Process.

13.2 The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:

13.2.1 immediately take all reasonable steps necessary to:

- (a) minimise the extent of actual or potential harm caused by such Breach of Security;
- (b) remedy such Breach of Security to the extent possible;
- (c) apply a tested mitigation against any such Breach of Security; and
- (d) prevent a further Breach of Security in the future which exploits the same root cause failure;

13.2.2 as soon as reasonably practicable and, in any event, within twelve (12) hours following the Breach of Security or attempted Breach of Security, the Supplier must provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis as required by the Buyer.

13.3 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors and/or all or any part of the

Information Management System, with this Call-Off Contract, then such remedial action shall be undertaken and completed at no additional cost to the Buyer.

14. Security Monitoring and Reporting

14.1 The Supplier shall:

- 14.1.1 monitor the delivery of assurance activities;
- 14.1.2 maintain and update the Security Management Plan in accordance with Paragraph 1;
- 14.1.3 agree a document which presents the residual security risks to inform the Buyer's decision on whether or not to give Approval to the Supplier to Process, store and transit the Government Data;
- 14.1.4 monitor security risk impacting upon the operation of the Service;
- 14.1.5 report Breaches of Security in accordance with the approved Incident Management Process; and
- 14.1.6 agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within 30 days of the Start Date of this Call-Off Contract.

Part C Accreditation requirements

1. This Part sets out:

- 1.1 The Accreditation arrangements that the Supplier must implement and comply with when providing the Services and performing its other obligations under this Call-Off Contract. These are required to ensure the security of the Government Data, the ICT Environment, the Services and the Information Management System, which are in addition to the requirements set-out in Parts A, B and E and Appendix 1 and 2 of this Schedule.
- 1.2 To facilitate the Supplier's design, implementation, operation, management and continual improvement of the Security Management Plan and the security of the Services and Information Management System and otherwise.
- 1.3 The Supplier shall provide access to the Supplier Staff responsible for information assurance and the Buyer shall provide access to its Personnel responsible for information assurance, at reasonable times upon reasonable written notice.

2. Information Management System

- 2.1. The Information Management System comprises the Core Information Management System and the Wider Information Management System.
- 2.2. The Buyer shall be responsible for determining the boundary between the Core Information Management System and the Wider Information Management System. In order to enable the Buyer to make such determination, the Supplier shall provide the Buyer with such documentation and information that the Buyer may reasonably require regarding any information assets, ICT systems and/or Sites which will be used by the Supplier or any Subcontractor to Process Government Data together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources). The Buyer shall notify the Supplier, as soon as reasonably practical following the receipt of such documentation and information, of its

decision regarding the component parts of the Core Information Management System and its boundary with the Wider Information Management System.

2.3. The Supplier shall reproduce the Buyer's decision as a diagram documenting the Core Information Management System, the Wider Information Management system and the boundary between the two. This diagram shall form part of the Security Management Plan.

2.4. Any proposed change to the component parts of the Core Information Management System or the boundary between the Core Information Management System and the Wider Information Management System shall be notified and processed in accordance with Clause 24 of the Core Terms (Changing the contract).

3. **Statement of Information Risk Appetite and Security Requirements**

3.1. The Supplier acknowledges that the Buyer has provided and the Supplier has received a statement of information risk appetite for the Supplier System and the Services ("**Statement of Information Risk Appetite**").

3.2. The Buyer's Security Requirements in respect of the Core Information Management System shall be set out in Appendix 1 (below).

4. **Accreditation of the Core Information Management System**

4.1. The Core Information Management System shall be subject to Accreditation in accordance with this Paragraph 4.

4.2. The Supplier acknowledges that the purpose of Accreditation is to ensure that:

4.2.1. the Security Management Plan accurately represents the Core Information Management System;

4.2.2. the Accreditation Plan, if followed, provides the Buyer with sufficient confidence that the CIMS will meet the requirements of the Security Requirements and the Statement of Risk Appetite; and

4.2.3. the residual risks of the Core Information Management System are no greater than those provided for in the Statement of Risk Appetite and Security Requirements.

4.3. The Accreditation shall be performed by the Buyer or by representatives appointed by the Buyer.

4.4. In addition to any obligations imposed by Call-Off Schedule 13 (Implementation Plan and Testing), the Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Subcontractors, from the Call-Off Contract Start Date.

4.5. By the date specified in the Implementation Plan, the Supplier shall prepare and submit to the Buyer the risk management documentation for the Core Information Management System, which shall be

subject to approval by the Buyer in accordance with, Part B Paragraph 5 (the "**Security Management Plan**").

- 4.6. The Supplier must provide, by the date by which the Supplier is required to have received a Risk Management Approval Statement from the Buyer together with:
 - 4.6.1. details of each of the tasks which must be completed by the Supplier, Milestones which must be Achieved and the Buyer responsibilities which must be completed in order for the Supplier to receive a Risk Management Approval Statement pursuant to Paragraph 4.8.1.
 - 4.6.2. a formal risk assessment of the Core Information Management System and a risk treatment plan for the Core Information Management System;
 - 4.6.3. a completed ISO 27001:2013 Statement of Applicability for the Core Information Management System; the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Services, processes associated with the delivery of the Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to extent that it is under the control of or accessed the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services; and
 - 4.6.4. unless such requirement is waived by the Buyer, proposed controls that will be implemented in respect of all aspects of the Services and all processes associated with the delivery of the Services, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Confidential Information of the Buyer and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Call-Off Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services including:
 - 4.6.4.1. the Required Changes Register;
 - 4.6.4.2. evidence that the Supplier and each applicable Subcontractor is compliant with the Certification Requirements;
 - 4.6.4.3. a Personal Data Processing Statement; and
 - 4.6.4.4. the diagram documenting the Core Information Management System, the Wider Information Management System and the boundary between the two created under Paragraph 3.2.
- 4.7. To facilitate Accreditation of the Core Information Management System, the Supplier shall provide the Buyer and its authorised representatives with:
 - 4.7.1. access to the Sites, ICT information assets and ICT systems within the Core Information Management System on request or in accordance with the Accreditation Plan; and
 - 4.7.2. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require, to enable the Buyer to establish that the Core Information Management System is compliant with the Security Management Plan.
- 4.8. The Buyer shall, by the relevant date set out in the Accreditation Plan, review the Security Management Plan and issue to the Supplier either:
 - 4.8.1. a Risk Management Approval Statement which will then form part of the Security Management Plan, confirming that the Buyer is satisfied that the identified risks to the Core Information

Management System have been adequately and appropriately addressed and that the residual risks are understood and accepted by the Buyer; or

- 4.8.2. a rejection notice stating that the Buyer considers that the identified risks to the Core Information Management System have not been adequately or appropriately addressed or the residual risks to the Core Information Management System have not been reduced to the level anticipated by the Statement of Information Risk Appetite, and the reasons why ("**Risk Management Rejection Notice**").
- 4.9. If the Buyer issues a Risk Management Rejection Notice, the Supplier shall, within 20 Working Days of the date of the Risk Management Rejection Notice:
 - 4.9.1. address all of the issues raised by the Buyer in such notice;
 - 4.9.2. update the Security Management Plan, as appropriate, and
 - 4.9.3. notify the Buyer that the Core Information Management System is ready for an Accreditation Decision.
- 4.10. If the Buyer issues a two or more Risk Management Rejection Notices, the failure to receive a Risk Management Approval Statement shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.
- 4.11. Subject to Paragraph 4.10, the process set out in Paragraphs 4.9 shall be repeated until such time as the Buyer issues a Risk Management Approval Statement to the Supplier or terminates this Call-Off Contract.
- 4.12. The Supplier shall not use the Core Information Management System to Process Government Data prior to receiving a Risk Management Approval Statement.
- 4.13. The Supplier shall keep the Core Information Management System and Security Management Plan under review and shall update the Security Management Plan annually in accordance with this

Paragraph 4 and the Buyer shall review the Accreditation Decision annually and following the occurrence of any of the events set out in Paragraph 4.9.

- 4.14. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
- 4.14.1. a significant change to the components or architecture of the Core Information Management System;
 - 4.14.2. a new risk or vulnerability is identified to the components or architecture of the Core Information Management System;
 - 4.14.3. a change in the threat profile;
 - 4.14.4. a Subcontractor failure to comply with the Core Information Management System code of connection;
 - 4.14.5. a significant change to any risk component; and/or
 - 4.14.6. a significant change in the quantity of Personal Data held within the Core Information Management System.
- 4.15. Where the Supplier has previously Processed Personal Data that does not include Special Category Personal Data, it starts to Process Special Category Personal Data, other than data relating to accessibility or dietary requirements relating to an individual:
- 4.15.1. a proposal to change any of the Sites from which any part of the Services are provided; and
 - 4.15.2. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns; and
 - 4.15.3. update the Required Changes Register and provide the updated Required Changes Register to the Buyer for review and Approval within 10 Working Days after the initial notification or such other timescale as may be agreed with the Buyer.
- 4.16. If the Supplier fails to implement a change which is set out in the Required Changes Register by the date agreed with the Buyer, such failure shall constitute a material Default and the Supplier shall:
- 4.16.1. immediately cease using the Core Information Management System to Process Government Data until the Default is remedied, unless directed otherwise .by the Buyer in writing and then it may only continue to Process Government Data in accordance with the Buyer's written directions; and
 - 4.16.2. where such Default is capable of remedy, the Supplier shall remedy such Default within the timescales set by the Buyer and, should the Supplier fail to remedy the Default within such timescales, the Buyer may terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms
- 4.17. The Supplier shall review each Change request against the Security Management Plan to establish whether the documentation would need to be amended should such Change request be agreed and, where a Change request would require an amendment to the Security Management Plan, the Supplier shall set out any proposed amendments to the documentation in the Impact Assessment associated with such Change request for consideration and Approval by the Buyer.
- 4.18. The Supplier shall be solely responsible for the costs associated with developing and updating the Security Management Plan and carrying out any remedial action required by the Buyer as part of the Accreditation process.

5. **Security Testing**

- 5.1. The Supplier shall, at its own cost and expense:
 - 5.1.1. procure testing of the Core Information Management System by a CHECK Service Provider (an "**IT Health Check**"):
 - 5.1.1.1. prior to it submitting the Security Management Plan to the Buyer for an Accreditation Decision;
 - 5.1.1.2. if directed to do so by the Buyer; and
 - 5.1.1.3. once every 12 Months during the Call-Off Contract Period;
 - 5.1.1.4. conduct vulnerability scanning and assessments of the Core Information Management System Monthly;
 - 5.1.1.5. conduct an assessment as soon as reasonably practicable following receipt by the Supplier or any of its Subcontractors of a critical vulnerability alert from a supplier of any software or other component of the Core Information Management System to determine whether the vulnerability affects the Core Information Management System; and
 - 5.1.1.5.1. conduct such other tests as are required by:
 - 5.1.1.5.2. any Vulnerability Correction Plans;
 - 5.1.1.5.3. the ISO27001 certification requirements;
 - 5.1.1.5.4. the Security Management Plan; and
 - 5.1.1.5.5. The Buyer following a Breach of Security or a significant change to the components or architecture of the Core Information Management System,
 - (each a "**Security Test**").
- 5.2. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within 10 Working Days, after completion of each Security Test.
- 5.3. In relation to each IT Health Check, the Supplier shall:
 - 5.3.1. agree with the Buyer the aim and scope of the IT Health Check;
 - 5.3.2. promptly, and in any case no later than 10 Working Days, following receipt of each IT Health Check report, provide the Buyer with a copy of the IT Health Check report
 - 5.3.3. in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
 - 5.3.4. prepare a remedial plan for approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:
 - 5.3.4.1. how the vulnerability will be remedied;
 - 5.3.4.2. the date by which the vulnerability will be remedied;
 - 5.3.4.3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;

- 5.3.4.4. comply with the Vulnerability Correction Plan; and
- 5.3.4.5. conduct such further Security Tests on the Core Information Management System as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.
- 5.4. The Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.
- 5.5. The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. Without prejudice to the Supplier's obligations under Paragraph 5.3, the Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case no later than 10 Working Days, after completion of each Security Test.
- 5.6. The Buyer and/or its authorised representatives shall be entitled, at any time and without giving notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the Service, the Information Management System and/or the Supplier's compliance with the Security Management Plan ("**Buyer Security Tests**"). The Buyer shall take reasonable steps to notify the Supplier prior to carrying out such Buyer Security Test to the extent that it is reasonably practicable for it to do so taking into account the nature and purpose of the Buyer Security Test.
- 5.7. The Buyer shall notify the Supplier of the results of such Buyer Security Tests after completion of each Buyer Security Test.
- 5.8. The Buyer Security Tests shall be designed and implemented so as to minimise their impact on the delivery of the Services. If a Buyer Security Test causes Supplier Non-Performance, the Buyer Security Test shall be treated as an Authority Cause for the purposes of Clause 5.1 of the Core Terms, except where the root cause of the Supplier Non-Performance was a weakness or vulnerability exposed by the Buyer Security Test.
- 5.9. Without prejudice to the provisions of Paragraph 5.3, where any Security Test carried out pursuant to this Paragraph 5 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the Core Information Management System and/or the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's Approval, the Supplier shall implement such changes to the Core Information Management System and/or the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible.
- 5.10. If the Buyer unreasonably withholds its Approval to the implementation of any changes proposed by the Supplier to the Security Management Plan in accordance with Paragraph 5.9 above, the Supplier shall not be deemed to be in breach of this Call-Off Contract to the extent it can be shown that such breach:
 - 5.10.1. has arisen as a direct result of the Buyer unreasonably withholding its Approval to the implementation of such proposed changes; and
 - 5.10.2. would have been avoided had the Buyer given its Approval to the implementation of such proposed changes.
- 5.11. For the avoidance of doubt, where a change to the Core Information Management System and/or the Security Management Plan is required to remedy non-compliance with the Risk Management Documentation, the Security Requirements and/or any obligation in this Call-Off Contract, the Supplier shall effect such change at its own cost and expense.

- 5.12. If any repeat Security Test carried out pursuant to Paragraph 5.3 reveals an actual or potential Breach of Security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default and the Buyer may terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.
- 5.13. The Supplier shall, by 31 March of each Financial Year during the Call-Off Contract Period, provide to the Buyer a letter from its chief executive officer (or equivalent officer) confirming that having made due and careful enquiry:
 - 5.13.1. the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters under this Call-Off Contract; and
 - 5.13.2. the Supplier is confident that its security and risk mitigation procedures with respect to the Services remain effective.
- 6. Vulnerabilities and Corrective Action
 - 6.1. In addition to the requirements within Part B, the Supplier shall:
 - 6.1.1. implement a mechanism for receiving, analysing and acting upon threat information supplied by NCSC, or any other competent Central Government Body;
 - 6.1.2. promptly notify NCSC of any actual or sustained attempted Breach of Security;
 - 6.1.3. ensure that the Core Information Management System is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
 - 6.1.4. ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Core Information Management System by actively monitoring the threat landscape during the Call-Off Contract Period;
 - 6.1.5. pro-actively scan the Core Information Management System for vulnerable components and address discovered vulnerabilities through the processes described in the Security Management Plan;
 - 6.1.6. from the date specified in the Accreditation Plan and within 5 Working Days of the end of each subsequent Month during the Call-Off Contract Period, provide the Buyer with a written report which details both patched and outstanding vulnerabilities in the Core Information Management System, the elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report and any failure to comply with the timescales set out in Part B Paragraph 5.4 for applying patches to vulnerabilities in the Core Information Management System;
 - 6.1.7. propose interim mitigation measures to vulnerabilities in the Core Information Management System known to be exploitable where a security patch is not immediately available;
 - 6.1.8. remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Core Information Management System); and
 - 6.1.9. inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Core Information Management System and provide initial indications of possible mitigations.
 - 6.2. If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under Part B Paragraph 5.4, the Supplier shall immediately notify the Buyer.

- 6.3. If the Supplier fails to patch vulnerabilities in the Core Information Management System in accordance with Part B Paragraph 5.3, such failure shall constitute a material Default and the Buyer may by terminate this Call-Off Contract with immediate effect by issuing a Termination Notice to the Supplier in accordance with Clause 10.4 of the Core Terms.

PART D Assurance requirements

1. This Part D sets out the Assurance arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Call-Off Contract to ensure the security of the Government Data and the Information Management System.
- 1.1 The Supplier must comply with the Assurance arrangements in addition to the other Security Requirements as set out within Parts A and B and E of this Schedule and Appendix 1 (Security Management Plan).
2. **Information Security Approval Statement**
- 2.1 The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Call-Off Schedule 9 (Security Requirements), including any requirements imposed on Sub-contractors from the Call-Off Start Date.
- 2.2 The Supplier may not use the Information Management System to Process Government Data unless and until:
 - 2.2.1 the Supplier has procured the conduct of an ITHC of the Supplier System by a CHECK Service Provider in accordance with Paragraph 4; and
 - 2.2.2 the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this Paragraph 2.
- 2.3 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule and the Call-Off Contract in order to ensure the security of the Government Data and the Information Management System.
- 2.4 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which comprises:
 - 2.4.1 an Information Assurance Assessment;
 - 2.4.2 the Required Changes Register;
 - 2.4.3 the Personal Data Processing Statement; and
 - 2.4.4 the Incident Management Process.
- 2.5 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:
 - 2.5.1 an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Government Data; or
 - 2.5.2 a rejection notice which shall set out the Buyer's reasons for rejecting the Security Management Plan.

- 2.6 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Buyer's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within 10 Working Days or such other timescale as agreed with the Buyer.
- 2.7 The Buyer may require and the Supplier shall provide the Buyer and its authorised representatives with:
- 2.7.1 access to the Supplier Staff;
 - 2.7.2 access to the Information Management System to Audit the Supplier and its Subcontractors' compliance with this Call-Off Contract;
 - 2.7.3 such other information and/or documentation that the Buyer or its authorised representatives may reasonably require;
 - 2.7.4 assistance to the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan; and
 - 2.7.5 the Supplier shall provide the access required by the Buyer in accordance with this Paragraph within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.
3. **Compliance Reviews**
- 3.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.
- 3.2 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
- 3.2.1 a significant change to the components or architecture of the Information Management System;
 - 3.2.2 a new risk to the components or architecture of the Service;
 - 3.2.3 a vulnerability to the components or architecture of the Service which is classified '**Medium**', '**High**', '**Critical**' or '**Important**' in accordance with the classification methodology set out in Paragraph 5 of Part B to this Schedule;
 - 3.2.4 a change in the threat profile;
 - 3.2.5 a significant change to any risk component;
 - 3.2.6 a significant change in the quantity of Personal Data held within the Service;
 - 3.2.7 a proposal to change any of the Sites from which any part of the Services are provided; and/or
 - 3.2.8 an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.
- 3.3 Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Required Changes Register and submit the updated Required Changes Register the Buyer for review and Approval.

- 3.4 Where the Supplier is required to implement a change, including any change to the Information Management System the Supplier shall effect such change at its own cost and expense.
4. **Security Testing**
- 4.1 The Supplier shall, at its own cost and expense procure and conduct:
- 4.1.1 testing of the Information Management System by a CHECK Service Provider ("ITHC"); and
 - 4.1.2 such other security tests as may be required by the Buyer; and
 - 4.1.3 the Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Buyer for review in accordance with Paragraph 3; and it shall repeat the ITHC not less than once every 12 Months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.
- 4.2 In relation to each ITHC, the Supplier shall:
- 4.2.1 agree with the Buyer the aim and scope of the ITHC;
 - 4.2.2 promptly, and no later than 10 Working Days, following the receipt of each ITHC report, provide the Buyer with a copy of the full report;
 - 4.2.3 in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
 - (a) prepare a remedial plan for Approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the ITHC report:
 - (i) how the vulnerability will be remedied;
 - (ii) the date by which the vulnerability will be remedied; and
 - (iii) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (b) comply with the Vulnerability Correction Plan; and
 - (c) conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.
- 4.3 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.
- 4.4 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique] that has the potential to affect the security of the Information Management System, the Supplier shall within days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:
- 4.4.1 propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and
 - 4.4.2 where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.

- 4.5 The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Schedule and the Call-Off Contract.
- 4.6 The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in Paragraph 5 of Part B to this Schedule.

Part E Certification requirements

Certification Requirements

- 1. Supplier Requirements
 - 1.1. The Supplier shall as applicable to the Lot and the associated Security Tier, ensure, at all times during the Call-Off Contract Period, that it is certified as compliant with:
 - 1.1.1. ISO/IEC 27001:2013 by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
 - 1.1.2. Cyber Essentials or Cyber Essentials PLUS as applicable to the Lot and Security Tier of the Service, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme), and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier or the relevant Subcontractor (as applicable) shall be permitted to use the Core Information Management System to receive, store or Process any Government Data.
- 2. **Payment Card Industry Data Security Standard (PCI DSS) Compliance**
 - 2.1. All Suppliers and / or Subcontractors that are a payment processor must be, and remain, appropriately certified according to the Payment Card Industry Data Security Standard requirements throughout the term of the Contract
 - 2.2. Where the Supplier and / or Subcontractor intends to accept payments, restricted to at sale only, by debit/credit card the Supplier and / or Subcontractor must have either:
 - 2.2.1. been certified by a Qualified Security Assessor as being compliant with the PCI DSS version 1.1;
 - 2.2.2. completed an internal self-assessment and will adhere at all times to the terms of the PCI DSS and will notify the Client promptly in writing of any changes in the Contractor's certification.
 - 2.3. The Supplier / Subcontractor must validate compliance in the manner deemed appropriate by the card scheme industry on an annual basis and provide the Buyer with written evidence of compliance annually.
 - 2.4. The Supplier / Subcontractor will be responsible for any costs incurred to attain and maintain compliance with PCI DSS.
 - 2.5. The Supplier / Subcontractor must meet all PCI DSS requirements, on a continuing basis, including but not limited to any subsequent versions of the PCI DSS.
 - 2.6. The Supplier / Subcontractor must be responsible for the security of all cardholder Data in their possession and must protect data by the card scheme industry standard on an annual basis and provide the Buyer access hosted environment and data when necessary.

- 2.7. The Supplier / Subcontractor must notify the Buyer and the card scheme industry immediately if it knows or suspects that there has been, or will be, a breach of the security of Cardholder Data or of the PCI DSS.
- 2.8. The Supplier / Subcontractor must indemnify the Buyer, its subsidiaries, affiliates, officers, employees and agents from and against all actions, demands, costs, Losses, whatsoever incurred by it or them arising out of or in connection with the Supplier's non-compliance with, or breach of, the PCI DSS or breach of Cardholder Data security.
- 2.9. The Supplier / Subcontractor must cease taking payments, by Debit Card / Credit Card, on behalf of the Buyer in the event that the Supplier becomes non-compliant with, or suffers a breach of, the PCI DSS or breach of Cardholder Data security.

3. **Subcontractor Requirement**

- 3.1. Notwithstanding anything else in this Contract, a CMIS Subcontractor shall be treated for all purposes as a Key Subcontractor.
- 3.2. In addition to the obligations contained in Joint Schedule 6 (Key Subcontractors), the Supplier must ensure that the Key Subcontract with each CIMS Subcontractor.
- 3.3. contains obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under this Call-Off Schedule 9 (Security Requirements);
 - 3.3.1. provides for the Buyer to perform Accreditation of any part of the Core Information Management System that the CIMS Subcontractor provides or operates which is not otherwise subject to Accreditation under this Call-Off Schedule 6 (Security Requirements).
- 3.4. The Supplier shall ensure that each Higher Risk Subcontractor is certified as compliant, and the Supplier shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data, with either:
 - 3.4.1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or
 - 3.4.2. Cyber Essentials PLUS, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme),
- 3.5. The Supplier shall ensure that each Medium Risk Subcontractor is certified compliant with Cyber Essentials, in accordance with the requirements in Framework Schedule 9 (Cyber Essentials Scheme).
- 3.6. The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Subcontractor shall:
 - 3.6.1. immediately ceases using the Government Data; and
 - 3.6.2. procure that the relevant Subcontractor promptly returns, destroys and/or erases the Government Data in accordance with Security Requirements.
- 3.7. The Buyer may agree to exempt, in whole or part, the Supplier or any Subcontractor from the Certification Requirements. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

Appendix 1

Security Management Plan Template

To be developed by the Supplier and agreed between the parties within the 1st month of the contract term.

Appendix 2

Accreditation - Core Information Management System diagram

To be developed by the Supplier and agreed between the parties within the 1st month of the contract term.

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

"Exclusive Assets"	1 Supplier Assets used exclusively by the Supplier in the provision of the Deliverables;
"Exit Information"	2 has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	3 the person appointed by each Party to manage their respective obligations under this Schedule;
"Exit Plan"	4 the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
"Net Book Value"	5 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"	6 those Supplier Assets used by the in connection with the Deliverables but which are also used by the Supplier for other purposes;
"Registers"	7 the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	8 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"	9 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"	10 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"	11 has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	12 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"	13 Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	14 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"	15 has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	16 has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for contract exit

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

2.2 During the Contract Period, the Supplier shall promptly:

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

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

("Registers").

2.3 The Supplier shall:

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

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

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

3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

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

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

4.4 The Supplier shall:

- a) maintain and update the Exit Plan (and risk management plan) no less frequently than: 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
- e) 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 (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 12 (Clustering)

1. Definitions

- 1.1 **"Cluster Members"** means a person named as such in the Annex A to this Schedule which shall be incorporated into the Order Form.

2. When you should use this Schedule

- 2.1 This Schedule is required where various Other Contracting Authorities want to join with the Buyer to efficiently contract collectively under a single Call Off Contract rather than as separate individual Buyers under separate Call Off Contracts.
- 2.2 A Buyer may add Cluster Members during the Call-Off Contract Period by complying with Clause 24 (Changing the Contract) of the Core Terms and the Regulations.

3. Cluster Members benefits under the Contract

- 3.1 The Buyer has entered into this Call-Off Contract both for its own benefit and for the benefit the Cluster Members.
- 3.2 The Cluster Members who are to benefit under the Call-Off Contract are identified Annex A to this Schedule.
- 3.3 Cluster Members shall have all of the rights granted to the Buyer under a Call-Off Contract. Accordingly, where the context requires in order to assure the Cluster Members rights and benefits under a Call-Off Contract, and unless the Buyer otherwise specifies, references to the Buyer in a Call-Off Contract (including those references to a Party which are intended to relate to the Buyer) shall be deemed to include a reference to the Cluster Members.
- 3.4 Each of the Cluster Members will be a third party beneficiary for the purposes of the CRTPA and may enforce the relevant provisions of a Call-Off Contract pursuant to CRTPA.
- 3.5 The Parties to a Call-Off Contract may in accordance with its provisions vary, terminate or rescind that Call-Off Contract or any part of it, without the consent of any Cluster Member.
- 3.6 The enforcement rights granted to Cluster Members under Paragraph 3.4 are subject to the following provisions:
- 3.6.1 the Buyer may enforce any provision of a Call-Off Contract on behalf of a Cluster Member;
- 3.6.2 any claim from a Cluster Member under the CRTPA to enforce a Call-Off Contract shall be brought by the Buyer if reasonably practicable for the Buyer and Cluster Member to do so; and
- 3.6.3 the Supplier's limits and exclusions of liability in the Call-Off Contract shall apply to any claim to enforce a Call-Off Contract made by the Buyer on behalf of a Cluster Member and to any claim to enforce a Call-Off Contract made by a Cluster Member acting on its own behalf.

- 3.7 Notwithstanding that Cluster Members shall each receive the same Services from the Supplier the following adjustments will apply in relation to how the Call-Off Contract will operate in relation to the Buyer and Cluster Members:
- 3.7.1 Services will be provided by the Supplier to each Cluster Member and Buyer separately;
 - 3.7.2 the Supplier's obligation in regards to reporting will be owed to each Cluster Member and Buyer separately;
 - 3.7.3 the Buyer and Cluster Members shall be entitled to separate invoices in respect of the provision of Deliverables;
 - 3.7.4 the separate invoices will correlate to the Deliverables provided to the respective Buyer and Cluster Members;
 - 3.7.5 the Charges to be paid for the Deliverables shall be calculated on a per Cluster Member and Buyer basis and each Cluster Member and the Buyer shall be responsible for paying their respective Charges;
 - 3.7.6 [NOT USED]
 - 3.7.7 such further adjustments as the Buyer and each Cluster Member may notify to the Supplier from time to time.
- 3.8 In order for a Cluster Member to benefit from the services under this Call-Off Contract, the Cluster Member must execute an engagement letter setting out details of their specific requirements for Deliverables ("**Engagement Letter**"). No school will be classed as a Cluster Member without an Engagement Letter.

Annex A – Cluster Members

The Deliverables shall also be provided for the benefit of the following Cluster Members:

Cluster Members	Services to be provided	Duration	Special Terms
Any school within England with a Unique Reference Number (URN)* - subject to execution of an Engagement Letter	See the following documents (listed in order of precedence): <ul style="list-style-type: none">- Signed Engagement Letter- Schedule 4 Call-off Tender- Schedule 20 Specification	As per Engagement Letter	As per Engagement Letter

*As found at <https://get-information-schools.service.gov.uk/Search?SelectedTab=Establishments&SearchType=ByLocalAuthority>

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

1. definitions

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

"Delay"	a) a delay in the Achievement of a Milestone by its Milestone Date; or b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	1 an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	2 a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	3 has the meaning given to it in Paragraph 7.1;

2. Agreeing and following the Implementation Plan

- 2.1** A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 10 days after the Call-Off Contract Start Date.
- 2.2** The draft Implementation Plan:
- 2.2.1 must cover all aspects of the Services and the Supplier's obligations under this Call-Off Contract, including the requirements set out in Call-off Schedule 9 (Security Management);
 - 2.2.2 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and
 - 2.2.3 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.
- 2.3** Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the

Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

- 2.4** The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.
- 2.5** The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

3. Reviewing and changing the Implementation Plan

- 3.1** Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.
- 3.2** The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.
- 3.3** Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.
- 3.4** Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

4. Security requirements before the Start Date

- 4.1** The Supplier shall note that it is incumbent upon them to understand and plan for the implementation of the Security Requirements applicable to the provision of the Services as detailed in Call-Off Schedule 9 (Security Management) which must be satisfied and in place before the Call-Off Start Date. The Supplier shall ensure that the applicable Security Requirements are reflected in their Implementation Plans.
- 4.2** The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's personnel security requirements set out in Paragraph 4.1 of Call-Off Schedule 9 (Security Management)-.
- 4.3** The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.
- 4.4** The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

- 4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.
- 4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5. What to do if there is a Delay

- 5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:
 - 5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;
 - 5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;
 - 5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and
 - 5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

6. Compensation for a Delay

- 6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:
 - 6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;
 - 6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:
 - (a) the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or
 - (b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

- 6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;
- 6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and
- 6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

Call-Off Schedule 14 (Service Levels)

1. Definitions

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Order Form;
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2. What happens if you don't meet the Service Levels

- 2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
- 2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.
- 2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.
- 2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:
- 2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or
- 2.4.2 the Service Level Failure:
- (a) exceeds the relevant Service Level Threshold;

- (b) has arisen due to a Prohibited Act or wilful Default by the Supplier;
- (c) results in the corruption or loss of any Government Data; and/or
- (d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and

2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

- 1.a.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- 1.a.2 instruct the Supplier to comply with the Rectification Plan Process;
- 1.a.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or
- 1.a.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

2.1 [NOT USED]

Annex A to Part A: Services Levels Table

Table 1 – Key Performance Indicators

Key Performance Indicators	Unit of Measure	Target	Reporting period
Education Setting Engagement Enquiries and referrals converted into commissioned activity	Engagement Letters signed and successful commissions	95% of all established contact with Education Settings to result in a commission	Monthly via pipeline reporting to the Department
Education Setting satisfaction Positive results of annual feedback form – Contents of form to be agreed with and signed off by the Department's contract manager	Feedback of "Good" or better	95% of all feedback returns reporting satisfaction of "Good" or better	Annual via feedback report
Social Value – Training Opportunities	Number of training opportunities (Level 2, 3, and 4+) created or retained by the supplier and engaged in this contract, other than apprentices, by UK region	2 opportunities to be created or retained per year	Annually via reporting to the Department

Table 2 – Service Levels

Service Level Description	Service Level Requirement
Enquiry Response	All Education Setting enquiries via the Supplier's helpdesk facility to be responded to within 1 working day
Enquiry Resolution	All Education Setting enquiries via the Supplier's helpdesk facility to be resolved within 5 working days

Call-Off Schedule 15 (Call-Off Contract Management)

Definitions

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;

Project Management

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.

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.

Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

Role of the Supplier Contract Manager

The Supplier's Contract Manager's shall be:

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;

able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

able to cancel any delegation and recommence the position himself; and

replaced only after the Buyer has received notification of the proposed change.

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.

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.

Role of the Operational Board

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.

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.

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.

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.

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.

Contract Risk Management

Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for: the identification and management of risks;

the identification and management of issues; and
monitoring and controlling project plans.

The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Call-Off Schedule 20 (Call-Off Specification)

SPECIFICATION

1. **Introduction**
 1. The Department is looking to drive value for money for the Education Sector by ensuring that schools can be assured that they are and have been billed accurately for their energy bills, which represent a significant proportion of their non-staff costs, whilst also supporting them by facilitating better access to their own data to help them manage and monitor their energy consumption.
2. **Background**
 1. There are currently circa 24,000 schools/academies across England, including Primary and Secondary phases. It is currently estimated that these institutions spend in excess of £1.3bn annually on utilities (Electricity and Gas).
 2. School budgets are under increasing pressure from increasing costs, in particular the significant recent increases in gas and electricity prices. Schools are looking to the Department for solutions for security of supply, budget certainty and energy efficient products and services to support reduction in energy consumption.
3. **Summary of the Requirement**
 1. The Supplier shall review utilities spend as required by the relevant Education Setting to identify, report and recover any amounts identified as overpaid, overcharged or erroneous.
 2. This Service shall be delivered directly to Education Settings in response to a commission via a Letter of Engagement. A copy of the form of Letter of Engagement can be found at Appendix A.
 3. The standard Service shall constitute the retrospective review of up to 6 years' worth of data from the date of commission for both electricity and gas – the time period being the default set by the Supplier unless otherwise agreed between the Supplier and Education Setting.
 4. The Supplier must ensure the Supplier is mobilised to deliver the Service from ~~1st July 2024~~ 1st September 2024.
 5. The Supplier shall not deliver any services beyond the contents of this Specification and is not required to make future contracting recommendations to the Education Setting.
4. **Service Methodology**
 1. Upon commissioning by an Education Setting– through a Letter of Engagement (see 6.2), the Supplier will liaise with the Education Setting to identify, obtain, review and cleanse the necessary utility billing data/documentation for review and establish points of contact for all necessary individuals within the Education Setting and associated Multi-Academy Trusts and/or Local Authorities.
 2. The Supplier shall conduct a thorough analysis of all identified data/documentation as part of the audit and identify any anomalies in charges, payments or agreements which have resulted in the Education Setting having missed, miscalculated, overpaid or been overcharged in respect of the relevant utilities by the Original Service Provider (“OSP”).
 3. The Supplier shall provide monthly updates to the Education Setting regarding progress of the audit.
 4. The Supplier shall report all findings from this audit to both the Department and the Education Setting upon completion including as a minimum the data specified in 7.1.

5. The Supplier shall present all findings including sums eligible for recovery to the Education Setting for authorisation prior to proceeding with the process of recovering these sums from the relevant OSP on behalf of the Education Setting.
 6. Authorisation must be provided by the Education Setting, through the completion of the authorisation template as set out in the CCS RM6226 framework (see Framework Schedule 1 Annex H), in order to proceed.
 7. On receipt of a signed authorisation form, the Supplier shall engage with the relevant OSP and agree recovery/repayment and methodology for doing so.
 8. The Supplier will effect recovery from the relevant OSP and provide the benefit of that recovery to the Education Setting.
 9. The Supplier will invoice for services provided based on a fixed percentage of monies recovered as agreed in the Contract (see Call-off Schedule 4 – Call-off Tender).
 10. 4.11. Subject to receipt by the Supplier of a completed data set as a result of engagement with the Education Setting, it is expected that these Services should be successfully completed in respect of the relevant Education Setting in a timescale set out in the Supplier's Contracted solution.
 11. If data is found to be incomplete, the Department expects the Supplier to work collaboratively with the Education Setting and OSP to rectify. The Supplier shall provide a monthly project update to the Department including ongoing activities and an indicative pipeline of future activities. This shall include information regarding the Education Settings, their review period, the cumulative value of their bills, the value of monies identified as recoverable, the recovery status and the payment made to the Supplier.
 12. The Supplier will seek feedback from all engaged Education Settings annually on the Services, utilising a form developed in conjunction with the Department and signed off by the Department's contract manager.
5. **Comms and Engagement**
1. The Supplier shall support the Department in launching a marketing campaign aimed at encouraging Education Settings to engage with the Contract and to undertake a utilities audit. This campaign is anticipated to have 2 stages:
 - a. Stage 1 – Targeted comms to the largest Multi-Academy Trusts (MATs) across England, with a total reach of approximately 1000 schools.
 - b. Stage 2 – National high-level comms and advertisement to all in-scope settings across England.
 2. The Supplier shall utilise any existing comms channels to assist with this campaign, however the Supplier must NOT make unsolicited calls to schools or participate in "cold calling" for engagement.
 3. To support the Department's marketing campaign, the Supplier shall run at least two promotional presentations in which the utilities audit process is explained and the sign-up/commissioning process is laid out. The dates of these seminars, to align with the anticipated marketing campaign and existing school term dates, are required to be:
 1. Wednesday 12th June 2024 [DATE TO BE REVISED]
 2. Wednesday 25th September 2024
 4. The Supplier shall provide all materials from the seminars in 5.3 to the Department, and shall permit them to be published on the Department's "Get help buying for schools" website for the duration of the Contract term.
 5. The Supplier will develop a case study utilising a worked activity by 31st December 2024 for publication on the Department's "Get help buying for schools" website.
 6. The Supplier will also be required to provide an enquiries/helpdesk facility for schools during standard office hours of 09:00-17:00 Monday to Friday. We would expect that this provision would be established utilising existing infrastructure to minimise costs under this Contract. This must be via a dedicated e-mail address or telephone helpline.

6. **Identification of Education Settings**
 1. Education Settings may take the form of an entire Multi-academy Trust or a standalone or small cluster of institutions.
 2. All Education Settings that express an interest in the Services and complete a Letter of Engagement are in scope of this activity, including those where minimal potential for money owed is identified. The Supplier must cost this risk into their pricing proposal at Tender, expressed as a Commission Price.
 3. The Supplier may NOT amend the Contract terms and conditions or the Commission Price or basis of payment as part of a Letter of Engagement.
7. **Data Requirements**
 1. Following analysis, the Supplier shall provide the following data to the respective Education Setting:
 1. meter number (e.g. MPAN/MPRN)
 2. meter serial number
 3. meter type (e.g. half hourly/non half hourly for electricity)
 4. third party supplier (i.e. third-party intermediary, if applicable)
 5. Third party charges/commission
 6. incumbent supplier
 7. contract period
 8. contract reference
 9. account number
 10. site name
 11. site address (supply address)
 12. charges breakdown
 - a. delivered cost of utility (total)
 - b. consumption charges
 - c. fixed/standing charges
 - d. KvA charges
 - e. VAT
 - f. CCL
 - g. other costs
 13. consumption breakdown
 14. consumption shown by month and year
 2. This data must also be provided in an aggregated format by the Supplier to the Department as part of a quarterly update.
 3. Above is the minimum data set, additional data fields may be requested and agreed at a later date subject to agreement by the Contract parties or between the Education Setting and the Supplier through the Letter of Engagement.
 4. Suppliers shall perform the role of independent data controller in relation to any personal data disclosed to the Supplier by the Education Setting.
 5. It is expected that very limited personal data will be required and/or made available for the execution of these Services (which is expected to be limited to contact details of relevant personnel at the Education Setting or its utility suppliers) and absolutely no student data will be disclosed to the Supplier at any time.
 6. Data supplied by the Education Setting cannot be used for any other purpose other than delivery of the Services stated above and under this Contract exclusively. Data cannot be stored beyond the term of the Contract. All data must be handled and destroyed in accordance with the terms of the Contract.
8. **Cost Model**

1. Charges will only be payable to the Supplier in the event that the provision of the Services results in the recovery of monies from the OSP and payment (or invoice credit) of such sums to the Education Setting.
2. The Charges for the Services shall be a Commission Price calculated as a percentage (%) of the gross monies received cumulatively under each Letter of Engagement by the Education Setting as a result of Supplier recovery.
3. The Supplier's Commission Price rate shall:
 1. be dependent on the value of monies collected. It is expected that the rate is lower, the higher the collection. This will take the form of bandings, for more information please see Annex 1 – Draft Call-off Terms and Annex 2 – Evaluation Criteria.
 2. not exceed the Supplier's standard Price rates set out in the framework agreement.
4. The rates must apply for the duration of the Contract and cover all Services stated in this Specification. The Supplier is not permitted to make any charge on a rate card basis or charge any fees to the Education Setting in addition to the charging mechanisms agreed in the Contract and this Specification.
5. Once the Education Setting has received the recovered funds, via invoice credit or otherwise agreed with the OSP, the Supplier shall submit an invoice to the Education Setting for their Commission Price.
9. **Service Levels & Key Performance Indicators (KPIs)**
 1. The Supplier will, as part of the Contract performance management process, be required to report monthly on progress towards meeting all KPIs.
 2. The table below sets out the Key Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.
 3. Please note that dates specified in the table may be subject to change prior to the Contract commencement date.
 4. The KPIs shall apply for the entire term of the Contract, unless otherwise agreed in writing between the parties.

Table 1 – Key Performance Indicators

See Call-off Schedule 14

Table 2 – Service Levels

See Call-off Schedule 14

Annex 1 to Joint Schedule 11 - Processing Personal Data

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

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are:

1.1.1.2 The contact details of the Supplier's Data Protection Officer are:

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

1.1.1.4 Any such further instructions shall be incorporated into 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> <ul style="list-style-type: none">- Personal data necessary for the fulfilling of the contracted services under this contract.
Duration of the Processing	<i>From the Start Date to the End Date of this contract unless extended under the terms, in which case the revised End Dte.</i>
Nature and purposes of the Processing	<p><i>The Processor will be required to collect, record and use personal data for the execution of its duties including the gathering of energy data from both the Cluster members (schools) and from the Original Service Providers (OSP) and for the co-ordination of the activity and execution of the audit and cost recovery.</i></p> <p><i>The Processor will also be required to destroy this data upon the End Date.</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>

	<i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i>
Type of Personal Data	<i>Names</i> <i>Telephone Numbers</i> <i>E-mail Addresses</i>
Categories of Data Subject	<i>School Staff (such as Office managers; School Business managers; teaching and leadership staff) as furnished by the Cluster Member.</i> <i>OSP Staff as furnished by the Cluster Member.</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	<i>All personal data must be destroyed within 1 (one) month of the End Date.</i>