FRAMEWORK SCHEDULE 6 (ORDER FORM TEMPLATE AND CALL-OFF SCHEDULES)

ORDER FORM

CALL-OFF REFERENCE: **Project_4499**

THE BUYER:	**THE SECRETARY OF STATE FOR EDUCATION**
BUYER ADDRESS	20 Great Smith St, Westminster, London SW1P 3BT
THE SUPPLIER:	**COMPUTACENTER (UK) LIMITED**
SUPPLIER ADDRESS:	Hatfield Ave, Hatfield, AL10 9TW
REGISTRATION NUMBER:	01584718
DUNS NUMBER:	22-602-3463
SID4GOV ID:	Not applicable

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated the date of last signature.

It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

1. Lot 2 Hardware & Associated Services

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) RM6068

3. The following Schedules in equal order of precedence:

    (a) Joint Schedules for RM6068

    Joint Schedule 2 (Variation Form)

    Joint Schedule 3 (Insurance Requirements)

    Joint Schedule 4 (Commercially Sensitive Information)

    Joint Schedule 6 (Key Subcontractors)

    Joint Schedule 10 (Rectification Plan)

    Joint Schedule 11 (Processing Data)

    Joint Schedule 12 (Supply Chain Visibility)

(b) Call-Off Schedules for Project_4499

Call-Off Schedule 1 (Transparency Reports)

Call-Off Schedule 5 (Pricing Details)

Call-Off Schedule 6 (ICT Services)

Call-Off Schedule 8 (Business Continuity & Disaster Recovery) Part A

Call-Off Schedule 9 (Security)

Call-Off Schedule 10 (Exit Management) Part A

Call-Off Schedule 13 (Implementation Plan and Testing)

Call-Off Schedule 14 (Service Levels)

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

Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.6)

5. Joint Schedule 5 (Corporate Social Responsibility) RM6068

6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

7. Annexes A to E Call-Off Schedule 6 (ICT Services)

8. The following Call Off Schedules shall not apply:

Call-Off Schedule 2 (Staff Transfer)

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Schedule 7 (Key Supplier Staff)

Call-Off Schedule 11 (Installation Works)

Call-Off Schedule 12 (Clustering)

Call-Off Schedule 17 (MOD Terms)

Call-Off Schedule 18 (Background Checks)

Call-Off Schedule 19 (Scottish Law)

Call-Off Schedule 21 (Northern Ireland Law)

Call-Off Schedule 22 (Lease Terms)

Call-Off Schedule 23 (Optional Provisions) Part [A/B]

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

CALL-OFF SPECIAL TERMS

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

Special Term 1: In this Call-Off Contract, unless the context otherwise requires, the following words shall have the following meanings:

Defined Term	**Meaning**
"Approved User"	a named contact within a Responsible Body who has been given delegated authority to place TechSource orders and approve support tickets on behalf of the Responsible Body;
"Bloatware"	unwanted software included on a new computer or mobile device by the manufacturer as agreed by the Buyer and Supplier;
"Buffer Volume"	the volume of Devices referred to in Special Term 6;
"Call-Off Initial Period"	the period commencing on the Call-Off Contract Start Date and ending on 31 March 2021;
"Cap"	the maximum number of Devices that a Responsible Body is entitled to order, as determined by the Buyer from time to time;
"Co-Design Process"	the process to be undertaken by the Buyer and the Supplier in accordance with Special Term 7;
"Delivery Contact"	the individual identified in the order placed on the Ordering Portal as the person to whom delivery of Devices should be made;
"Devices"	the equipment set in Annex A Part 1 of Schedule 5 (Pricing);
"Extension Period"	either of the Call-Off Optional Extension Periods referred to in this Call-Off Order Form;
"Imaged Device"	a Device which has security, settings and applications applied by the Supplier using methods provided by the Buyer;
"Key Contact"	the principal contact person of a Responsible Body or school, as the case may be, as notified on the Ordering Portal;
"Lockdown"	a local lockdown as a result of COVID-19 announced by HM Government and/or a full or partial school closure;
"Ordering Portal"	the ordering portal named TechSource established and maintained by the Supplier in relation to, inter alia, the Deliverables;

"Outline Implementation Plan"	the high level implementation plan set out in Annex 1 of Schedule 13 (Implementation Plan and Testing);
"Responsible Bodies"	Local Authorities, Multi Academy Trusts;
"Schools"	An education establishment to which Deliverables will be dispatched by the Supplier;
"Secured Device"	a Windows device with the Buyer's build applied and security to ensure that the build cannot be removed without the password supplied;
"Service Period"	a period of one Month;
"Support Portal"	the online portal available 24x7 for Key Contracts and Approved Users to initiate support requests;
Support Requests"	requests for support for the logging of technical support as set out in the Specification excluding the optional support requirements
"Test Plan"	a plan for the Testing of the Deliverables to demonstrate compliance with Contract requirements;
"Test Report"	a test report produced by the Supplier in accordance with Paragraph 3.3 of Part B to Call-Off Schedule 13;

Special Term 2: REDACTED.

Special Term 3: REDACTED.

Special Term 4: REDACTED.

Special Term 5:

Modern Slavery, Child Labour and Inhumane Treatment

1.1 The Supplier:

1.1.1 shall not use, or allow its Subcontractors to use, forced, bonded or involuntary prison labour;

1.1.2 shall not require any Supplier staff or Subcontractor staff to lodge deposits or identity papers with the Employer or deny Supplier staff freedom to leave their employer after reasonable notice;

1.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;

1.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world;

1.1.5 shall make reasonable enquiries to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world;

1.1.6 shall have and maintain throughout the Term of the Call-Off Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and shall include in its contracts with its subcontractors anti-slavery and human trafficking provisions;

1.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under this Call-Off Contract;

1.1.8 shall prepare and deliver to the Buyer within fourteen (14) days of the Start Date and updated on a frequency defined by the Department, a slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business;

1.1.9 shall not use, or allow its employees or Subcontractors to use, physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

1.1.10 shall not use, or allow its Subcontractors to use, child or slave labour;

1.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to the Buyer and Modern Slavery Helpline1.

Special Term 6: REDACTED.

Special Term 7: REDACTED.

Special Term 8: REDACTED.

CALL-OFF START DATE:	**30/07/2020**
CALL-OFF EXPIRY DATE:	**31/03/2021**
CALL-OFF INITIAL PERIOD:	**8 months and 1 day**
CALL-OFF OPTIONAL EXTENSION PERIOD	**2 periods of 6 months**

CALL-OFF DELIVERABLES

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

LOCATION FOR DELIVERY

The Buyer will inform the Responsible Bodies that they must provide a list of the locations for delivery to the Supplier.

The Buyer will inform the Responsible Bodies that full delivery information as reasonably required by the Supplier must be provided by the Responsible Bodies in advance of any Services being performed including: Contact address, contact name, and any relevant delivery restrictions.

[1] The "Modern Slavery Helpline" refers to the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

Title to Goods is transferred to the Buyer on payment of the invoice relating to such Goods.

DATES FOR DELIVERY OF THE DELIVERABLES

See details in Call-Off Schedule 13 (Implementation Plan & Testing).

TESTING OF DELIVERABLES

The Devices are provided with stated manufacturer warranty only.

See details in Call-Off Schedule 13 (Implementation Plan & Testing).

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be the duration of any guarantee or warranty period the Supplier has received from the third party manufacturer or supplier. The Buyer and Supplier will have the option to introduce an enhanced warranty service by way of contract variation in line with the charges set out in Schedule 5 (Pricing Schedule).

MAXIMUM LIABILITY

REDACTED

CALL-OFF CHARGES

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

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

The Supplier shall submit invoices directly to the billing address as per the Buyer's order. The Supplier shall invoice the Buyer for Goods and for Services in accordance with Call-Off Schedule 5 (Pricing Details). Payment to be made by BACS payment.

BUYER'S INVOICE ADDRESS:

REDACTED

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED

BUYER'S ENVIRONMENTAL POLICY Not applicable

BUYER'S SECURITY POLICY

See Call-Off Schedule 9 (Security)

SUPPLIER'S AUTHORISED REPRESENTATIVE

REDACTED

SUPPLIER'S CONTRACT MANAGER

REDACTED

PROGRESS REPORT FREQUENCY

See Call-Off Schedule 1 (Transparency Reports).

PROGRESS MEETING FREQUENCY

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

KEY STAFF

Not applicable

KEY SUBCONTRACTOR(S)

None

COMMERCIALLY SENSITIVE INFORMATION

See Joint Schedule 4 (Commercially Sensitive Information).

SERVICE CREDITS

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

ADDITIONAL INSURANCES

Not applicable.

GUARANTEE

Not applicable.

SOCIAL VALUE COMMITMENT

Not applicable.

For and on behalf of the Supplier:	**For and on behalf of the Buyer:**

Signature:	Signature:
Name:	Name:
Role:	Role:
Date:	Date:

JOINT SCHEDULE 2 (VARIATION FORM)

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

Contract Details		
This variation is between:	The Secretary of State for Education (**"the Buyer"**) And Computacenter (UK) Limited (**"the Supplier"**)	
Contract name:	Device Reserve – Get Help With Technology	
Contract reference number:	**Project_4499**	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by the Buyer**.**

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

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

Signed by an authorised signatory for and on behalf of the Buyer

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

JOINT SCHEDULE 4 (COMMERCIALLY SENSITIVE INFORMATION)

1. WHAT IS THE COMMERCIALLY SENSITIVE INFORMATION?

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

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

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

No.	Date	Item(s)	Duration of Confidentiality
	7th August 2020	Special Terms	REDACTED
		Maximum Liability clause	
		Joint Schedule 3 – Insurance Requirements	
		Joint Schedule 4 – Call Off Tender	
		Call Off Schedule 1 (Transparency Reports)	
		Call Off Schedule 5 (Pricing Details)	
		Call Off Schedule 8 (BCD) Annex 1	
		Call Off Schedule 13 (Implementation Plan and Testing) – Annex 1	
		Call Off Schedule 14 (Service Levels) - Definition of Critical Service Failure, Annex 1 to Section 2 (Service Levels and Service Credits)	
		Call Off Schedule 20 (Specification) – Annex A	

JOINT SCHEDULE 11 (PROCESSING DATA)

Status of the Controller

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

1.1 "Controller" in respect of the other Party who is "Processor";

1.2 "Processor" in respect of the other Party who is "Controller";

1.3 "Joint Controller" with the other Party;

1.4 "Independent Controller" of the Personal Data where the other Party is also "Controller",

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

Where one Party is Controller and the other Party its Processor

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

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

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

4.1 a systematic description of the envisaged Processing and the purpose of the Processing;

4.2 an assessment of the necessity and proportionality of the Processing in relation to the Services;

4.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

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

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

5.1 Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

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

5.2.1 nature of the data to be protected;

5.2.2 harm that might result from a Data Loss Event;

5.2.3 state of technological development; and

5.2.4 cost of implementing any measures;

5.3 ensure that :

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

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

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

(b) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

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

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

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

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

5.3.5 the Data Subject has enforceable rights and effective legal remedies;

5.3.6 the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

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

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

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

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

6.2 receives a request to rectify, block or erase any Personal Data;

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

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

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

6.6 becomes aware of a Data Loss Event.

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

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

8.1 the Controller with full details and copies of the complaint, communication or request;

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

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

8.4 assistance as requested by the Controller following any Data Loss Event; and/or

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

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

9.1 the Controller determines that the Processing is not occasional;

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

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

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

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

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

12.1 notify the Controller in writing of the intended Subprocessor and Processing;

12.2 obtain the written consent of the Controller;

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

12.4 provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

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

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

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

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

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

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

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 17 of this Joint Schedule 11, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

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

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

21.1 to the extent necessary to perform their respective obligations under the Contract;

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

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

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

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

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

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

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

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

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

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

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

26.1 implement any measures necessary to restore the security of any compromised Personal Data;

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

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

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

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

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

Annex 1 - Processing Personal Data

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

1. The contact details of the Relevant Authority's Data Protection Officer are: REDACTED

2. he contact details of the Supplier's Data Protection Officer are: REDACTED

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

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

Personal Data Processing

Description	Details
Identity of Controller for each Category of Personal Data	**1. The Relevant Authority is Controller and the Supplier is Processor.** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 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: (a) Information relating to the Responsible Bodies **2. The Relevant Authority is a joint controller with the Responsible Bodies and the Supplier is the Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority and the Responsible Bodies are Joint Data Controller and the Supplier is the Processor of the following Personal Data: (a) Data used to support the execution of the contract (b) Data used to capture an audit trail of activity (c) Data used to resolve any delivery or ordering processes and or dispute issues **3. The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: (a) Business contact details of Supplier Personnel for which the Supplier is the Controller (b) Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier

	Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller.
Duration of the Processing	12 months from contract signature.
Nature and purposes of the Processing	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. The purpose includes the ordering, setup, management, and updating, delivery and contracted support for the devices.
Type of Personal Data	Personal data processed for the purposes of supporting the execution of the contract, capturing an audit trail of activity, resolving ordering and delivery of devices, or contracted support for devices with Responsible Bodies; business contact details of Supplier Personnel or directors, officers, employees, agents and contractors of the Relevant Authority
Categories of Data Subject	Responsible Bodies and their staff (including volunteers, agents, and temporary workers). Responsible Bodies will be responsible for allocating devices to named individuals.
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**	Data would need to be held for 7 (seven) years for statutory financial purposes.

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 Within ten (10) days 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.

1.5 The information detailed in Annex A below is not a definitive or exhaustive final list. Any changes or additional reporting requirements will be agreed jointly prior to Contract commencement or as part of the co-design process to be undertaken by the Parties. In particular, the Parties will agree, acting reasonably and in good faith, the provision of reports in relation to requests for admin passwords, shared support performance reporting, Ordering Portal and Support Portal performance (including detail of numbers of queries and time to resolve), inbound logistics of Devices and details of current stock levels.

Annex A

List of Transparency Report

It is key to the Buyer that regular reporting as set out below is adhered to. The principles that the Buyer and the Supplier have agreed in relation to the key data required to demonstrate the performance of the Supplier is based on the following principles:

1. It is expected that Responsible Bodies will use the Support and Ordering portals for tracking and monitoring their incidents, requests and orders in line with the scope detailed within Schedule 20.

2. Schools are able to log support requests but will have no access to online reporting

Title	Content	Format	Freq.	Content Provided	Produced By:	Buyer Contact
Performance - Summary report by Responsible Body on its position in the process.	Report to measure where a school is on their user journey from Order to delivery	Excel electronic file to be downloaded via MS TEAMS reporting bridge	Daily (Daily unless no transactions have occurred)	To include as a minimum - vendor type - orders placed - orders fulfilled	Supplier	REDACTED
User Ordering and Support service usage	To identify and track user activity/ log-in to ensure ordering process is adhered throughout the ordering journey from initial invitation to place order through to fulfilment. Where REDACTED has been implemented and is used in the provision of the Service, the reporting shall only be in respect of that part of the User Ordering and Support Service provided by the Supplier	Excel electronic file to be downloaded via MS TEAMS reporting bridge	Weekly	To include as a minimum - confirmation of user Log-in to the Support Portal only by xx date - Process status in the Support Portal - Order placed date in the Ordering Portal - Order fulfilled by date from SAP ERP.	Supplier	REDACTED
Performance – Helpdesk performance in respect of those elements handled by a Supplier system.	Provide weekly report to the Buyer to provide an overview of the use of the helpdesk service showing performance against each of the following categories. Report should itemise the source, nature of the incident, action taken, time taken to inform the Responsible Body and time taken to resolve. Report also to include: Number of incidents/requests handled	Excel electronic file to be downloaded via MS TEAMS reporting bridge	Weekly	- Number of incidents/requests received - Responsible Body - User - Type - Time / Date Logged - Time / Date response - Time / Date Resolved - Status	Supplier	REDACTED

Performance - Daily "outstanding orders" report	List of live approved orders by Responsible Body showing order status of deliveries	Excel electronic file to be downloaded via MS TEAMS reporting bridge	Daily unless there has been no change.	List of live approved orders by Responsible Body showing order status of deliveries	Supplier	REDACTED
Performance – Orders completed	List of completed orders by Responsible Body	Excel electronic file to be downloaded via MS TEAMS reporting bridge	Daily	List of completed orders by Responsible Body including device breakdown and quantity	Supplier	REDACTED
Technical – ordering portal performance and support team in respect of those elements handled by a Supplier system.	To include a daily report of ordering portal uptime and outages and daily volumes of Responsible Body inquiry presented and answered	Excel electronic file to be downloaded via MS TEAMS reporting bridge	Daily	To include a daily report of portal uptime and outages when not 100% and daily volumes of Responsible Body inquiry presented and answered	Supplier	REDACTED

CALL-OFF SCHEDULE 5 (PRICING DETAILS)

1. CHARGES

1.1 The price for the hardware and associated services, detailed in Annex A below, is:

	Charge Component	Charge
1.1.1	**REDACTED**	**REDACTED**
1.1.2	**REDACTED**	**REDACTED**
1.1.3	**REDACTED**	**REDACTED**
1.1.4	**REDACTED**	**REDACTED**
1.1.5	**REDACTED**	**REDACTED**
1.1.6	**REDACTED**	**REDACTED**
	Total Charge	**REDACTED**

1.2 REDACTED.

2. INVOICING

2.1 The Supplier will invoice the Buyer for Devices REDACTED. This is subject to the Buy and Store terms as set out in Annex B and is based on the volume of Devices set out in Annex A.

2.2 The Supplier will submit invoices to the Buyer for Configuration (paragraph 1.1.2) REDACTED.

2.3 The Supplier will submit invoices to the Buyer for Delivery (paragraph 1.1.3) REDACTED.

2.4 The Supplier will submit invoices to the Buyer for the Services described in paragraph 1.1.4 REDACTED. REDACTEDREDACTEDREDACTED.

2.5 The Supplier will submit an invoice to the Buyer for the services described in paragraph 1.1.5 REDACTED.

2.6 The Supplier will submit any invoice(s) for paragraph 1.1.6 as jointly agreed by both Parties.

2.7 Invoices are payable on REDACTED from receipt of the invoice.

3. BUYER RESPONSIBILITIES

REFERENCE	Buyer's Responsibilities
D-001	REDACTED
D-002	REDACTED

D-003	REDACTED
D-004	REDACTED
D-005	REDACTED
D-006	REDACTED

4. ASSUMPTIONS

4.1 The Buyer acknowledges that the total Charges, approach and timescale are based on the following Assumptions and Parameters:

REFERENCE	ASSUMPTIONS AND PARAMETERS
A-001	REDACTED
A-002	REDACTED
A-003	REDACTED
A-004	REDACTED
A-007	REDACTED
A-008	REDACTED
A-009	REDACTED
A-0010	REDACTED
A-0011	REDACTED
A-0012	REDACTED
A-0013	REDACTED
A-0014	REDACTED
A-0015	REDACTED

A-0016	REDACTED
A-0020	REDACTED
A-0021	REDACTED
A-0022	REDACTED
A-0124	REDACTED
A-0125	REDACTED

4.2 In the event that the Buyer fails to perform any of the Buyer Responsibilities set out in paragraph 3 or any one or more of the Assumptions set out in paragraph 4.1 proves to be incorrect or where they change then the parties shall work together (acting reasonably and in good faith) to reduce the impact of this within the agreed timescales and estimated Charges and failing that then either:

4.2.1 The parties shall agree a Contract Change Notice to deal with the impact; or

4.2.2 The matter shall be referred to the Dispute Resolution Procedure.

5. ADDITIONAL INFORMATION

DESCRIPTION	INCLUDED IN CHARGES?
REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**
REDACTED	**REDACTED**

Annex A – Pricing Details

Part 1 – Devices

REDACTED

Delivery Schedule

REDACTED

Part 2 - Services

Service Description	Unit Price (where applicable)	Number of units	Maximum Price
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**
Total		**REDACTED**	**REDACTED**

The Supplier shall provide the following services REDACTEDto the Buyer: **REDACTED**

The below services are not included in the total – these are an option which the Department may choose to take up by way of variation during the Call-Off Initial Period as per the Supplier's tender response set out in Schedule 4 (Call-Off Tender)**:**

Optional Services	Unit Price (where applicable)	Number of units	Total Price
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**
REDACTED	**REDACTED**	**REDACTED**	**REDACTED**

REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

Annex B – Buy and Store Agreement

BUY AND STORE OR CUSTOMER OWNED KIT AGREEMENT

Enter Buyer's Name
Enter Buyer's Address

REDACTED

Yours sincerely

Enter your name

ACCEPTANCE OF TERMS AND CONDITIONS
Signed on behalf of: **Enter Customer Name**
.....
By signing above I confirm I am authorised to sign this Agreement on behalf of
Enter Customer Name

Date:
Full Name:
Position:
Group Finance Operations
Post Point 11
Computacenter (UK) Limited
Hatfield Avenue, Hatfield, Hertfordshire
AL10 9TW

CALL-OFF SCHEDULE 6 (ICT SERVICES)

1. DEFINITIONS

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

"Buyer Property"	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
"Buyer Software"	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
"Buyer System"	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Defect"	any of the following: (a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or (d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;
"Emergency Maintenance"	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;
"ICT Environment"	the Buyer System and the Supplier System;

"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors (if any) or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
"Maintenance Schedule"	has the meaning given to it in paragraph 8 of this Schedule;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"New Release"	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
"Open Source Software"	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
"Operating Environment"	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: (a) the Deliverables are (or are to be) provided; or (b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or (c) where any part of the Supplier System is situated;
"Permitted Maintenance"	has the meaning given to it in paragraph 8.2 of this Schedule;
"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;

"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor (if any) or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. WHEN THIS SCHEDULE SHOULD BE USED

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

3. BUYER DUE DILIGENCE REQUIREMENTS

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

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

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

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

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

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

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

3.2.2 the actions needed to remedy each such unsuitable aspect; and

3.2.3 a timetable for and the costs of those actions.

4. SOFTWARE WARRANTY

4.1 The Supplier represents and warrants that:

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

4.1.2 all components of the Specially Written Software shall:

(a) be free from material design and programming errors;

(b) perform in all material respects in accordance with the relevant specifications and Documentation; and

(c) not infringe any IPR.

5. PROVISION OF ICT SERVICES

5.1 The Supplier shall:

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

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

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

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

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

6. STANDARDS AND QUALITY REQUIREMENTS

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

6.2 The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

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

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

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

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

6.4.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT AUDIT

7.1 The Supplier shall allow any auditor access to the Supplier premises to:

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

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

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

8. MAINTENANCE OF THE ICT ENVIRONMENT

8.1 If specified by the Buyer undertaking a Further Competition, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer in accordance with the timetable and instructions specified by the Buyer. In relation to this paragraph, the Supplier's ICT Environment comprises the Supplier systems used for the provision of the Deliverables including the following : ServiceNow Support Portal, TechSource Ordering Portal and SAP Enterprise Resource Planning platform.

8.2 The Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

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

8.4 The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. INTELLECTUAL PROPERTY RIGHTS IN ICT

9.1 Assignments granted by the Supplier: Specially Written Software

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

(a) the Documentation, Source Code and the Object Code of the Specially Written Software; and

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

9.1.2 The Supplier shall:

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

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

(c) without prejudice to paragraph 9.1.2(b), provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

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

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

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

(a) of its own Existing IPR that is not COTS Software;

(b) third party software that is not COTS Software

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

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

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

(b) only use such third party IPR as referred to at paragraph 9.2.3 (a) if the Buyer Approves the terms of the licence from the relevant third party.

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

9.2.5 The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

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

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

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

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

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

(a) will no longer be maintained or supported by the developer; or

(b) will no longer be made commercially available

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

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

(a) a Central Government Body; or

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

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

9.5 **Licence granted by the Buyer**

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

9.6 **Open Source Publication**

9.6.1 Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

(a) suitable for publication by the Buyer as Open Source; and

(b) based on Open Standards (where applicable),

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

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

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

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

(c) do not contain any material which would bring the Buyer into disrepute;

(d) can be published as Open Source without breaching the rights of any third party;

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

(f) do not contain any Malicious Software.

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

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

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

9.7 **Malicious Software**

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

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

losses and to restore the provision of the Deliverables to its desired operating efficiency.

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

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

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

10. SUPPLIER-FURNISHED TERMS

10.1 Software Licence Terms

10.1.1 Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in Annex A of this Call-Off Schedule 6.

10.1.2 Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in Annex B of this Call-Off Schedule 6.

10.2 Software Support & Maintenance Terms

10.2.1 Additional terms for provision of Software Support & Maintenance Services are detailed in Annex C of this Call-Off Schedule 6.

10.3 Software as a Service Terms

10.3.1 Additional terms for provision of a Software as a Service solution are detailed in Annex D of this Call-Off Schedule 6.

10.4 Device as a Service Terms

10.4.1 Additional terms for provision of a Device as a Service solution are detailed in Annex E to this Call-Off Schedule 6;

10.4.2 Where Annex E is used the following Clauses of the Core Terms shall not apply to the provision of the Device as a Service solution:

Clause 8.7

Clause 10.2

Clause 10.3.2]

11. CUSTOMER PREMISES

11.1 Licence to occupy Customer Premises

11.1.1 Any Customer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Call- Off Contract. The Supplier shall have the use of such Customer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Call-Off Contract [and in accordance with Call-Off Schedule 10 (Exit Management)].

11.1.2 The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Call-Off Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

11.1.3 Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of this Call-Off Schedule 6 and set out in the Order Form (or elsewhere in this Call Off Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this paragraph 11.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

11.1.4 The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

11.1.5 The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

11.2 Security of Buyer Premises

11.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

11.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

12. BUYER PROPERTY

12.1 Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

12.2 The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

12.3 The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors (if any) and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

12.4 The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

12.5 The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with this Call-Off Contract and for no other purpose without Approval.

12.6 The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance with Call- Off Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

12.7 The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by a Buyer Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

13. SUPPLIER EQUIPMENT

13.1 Unless otherwise stated in this Call Off Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

13.2 The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

13.3 The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Call-Off Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

13.4 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

13.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Call Off Contract, including the Service Levels.

13.6 The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

13.7 The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

13.7.1 remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with this Call-Off Contract; and

13.7.2 replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

ANNEX A

Non-COTS Third Party Software Licensing Terms

The Supplier shall provide details of all Non-COTS Third Party Software Licensing Terms within ten (10) Working Days of contract signature.

ANNEX B

COTS Licensing Terms

Third party software (if any) shall be licensed subject to the third party licensor's standard license terms which shall govern the supply, the Customer's use of and obligations relating to the software in their entirety.

ANNEX C

Software Support & Maintenance Terms

Third party services (if any) shall be supplied subject to the applicable third party's standard service terms.

ANNEX D

Software as a Service Terms

Not in Use

ANNEX E

Device as a Service Terms

Not in use

CALL-OFF SCHEDULE 8 (BUSINESS CONTINUITY AND DISASTER RECOVERY)

1. DEFINITIONS

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

"BCDR Plan"	has the meaning given to it in Paragraph 2.1 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.3.2 of Part A of this Schedule;
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.3.3 of Part A of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.3 of Part A of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of Part A of this Schedule;

2. BCDR PLAN

2.1 The BCDR Plan provided by Supplier can be found in Annex 1 of this Call-Off Schedule 8 (**"BCDR Plan"**). Subject to Paragraph 2.2 of this Schedule 8, the Buyer has accepted the BCDR Plan provided by the Supplier set out in Annex 1.

2.2 The Supplier shall prepare and deliver to the Buyer for the Buyer's written approval an updated BCDR Plan, within ten (10) Working Days of the Call-Off Start Date which shall address any updates to the BCDR Plan reasonably requested by the Buyer including but not limited to detailing the processes and arrangements that the Supplier shall follow to:

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

2.2.2 the recovery of the Deliverables in the event of a Disaster.

2.3 The BCDR Plan shall be divided into three sections:

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

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

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

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

3. GENERAL PRINCIPLES OF THE BCDR PLAN (SECTION 1)

3.1 Section 1 of the BCDR Plan shall:

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

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

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

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

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

3.1.6 contain a risk analysis, including:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. BUSINESS CONTINUITY (SECTION 2)

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

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

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

4.2 The Business Continuity Plan shall:

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

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

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

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

5. DISASTER RECOVERY (SECTION 3)

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

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

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

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

5.2.4 loss of a Subcontractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

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

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

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

5.2.13 testing and management arrangements.

6. REVIEW AND CHANGING THE BCDR PLAN

6.1 The Supplier shall review the BCDR Plan:

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

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

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

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

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

6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties

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

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

7. TESTING THE BCDR PLAN

7.1 The Supplier shall test the BCDR Plan:

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

7.1.2 in the event of any major reconfiguration of the Deliverables

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

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

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

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

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

7.5.1 the outcome of the test;

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

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

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

8. INVOKING THE BCDR PLAN

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

9. CIRCUMSTANCES BEYOND YOUR CONTROL

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

10. COVID-19 GOVERNMENT GUIDANCE

10.1 In compliance with Government's COVID-19 distancing rules, BCDR related discussions between the Parties shall take place via a Virtual Meeting Platform. The preferred Virtual Meeting Platform will be the one proposed by the Buyer.

ANNEX 1

BCDR PLAN

REDACTED

CALL-OFF SCHEDULE 9 (SECURITY)

Commodity Service Security Requirements

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

["ISMS" means the information security management system and process developed by the Supplier in accordance with paragraph 2 (ISMS) as updated from time to time; and]

"Security Management Plan" means the Supplier's security management plan prepared pursuant to paragraph 2.

1. The Supplier will ensure that any Supplier system which holds any Buyer Data will comply with:

1.1 the Departmental Security Requirements (Annex 1)

1.2 the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications

1.3 guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets

1.4 the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection

1.5 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

1.6 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

2. If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's Approval of) a Security Management Plan [and an Information Security Management System]. After Buyer Approval the Security Management Plan [and Information Security Management System] will apply during the Term of this Call-Off Contract. The/Both plan[s] will protect all aspects and processes associated with the delivery of the Services.

3. The Supplier will immediately notify the Buyer of any breach of security of the Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer Confidential Information however it may be recorded.

4. Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

Annex 1: Departmental Security Requirements

12. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"CPA" "Commercial Product Assurance" [formerly called "CESG Product Assurance"]	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body
"Data" "Data Controller" "Data Protection Officer" "Data Processor" "Personal Data" "Personal Data requiring Sensitive Processing" "Data Subject", "Process" and "Processing"	shall have the meanings given to those terms by the Data Protection Act 2018
"Department's Data" "Department's Information"	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any

	of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
"DfE" "Department"	means the Department for Education
"Departmental Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
"Digital Marketplace / G-Cloud"	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
End User Devices	means the personal computer or consumer devices that store or process information.
"Good Industry Practice" "Industry Good Practice"	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"Good Industry Standard" "Industry Good Standard"	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" "GSCP"	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	means Her Majesty's Government
"ICT"	means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.

“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
“OFFICIAL” “OFFICIAL-SENSITIVE”	the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP). the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.
“RBAC” “Role Based Access Control”	means Role Based Access Control. A method of restricting a person’s or process’ access to information depending on the role or functions assigned to them.
“Storage Area Network” “SAN”	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
“Secure Sanitisation”	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
“Security and Information Risk Advisor” “CCP SIRA” “SIRA”	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
“Senior Information Risk Owner” “SIRO”	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for

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

12.1 The Contractor shall be aware of and comply the relevant HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

12.2 Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated; that "contractors supplying products or services to HMG shall have achieved, and will be expected to retain certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

12.3 Where clause 12.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

12.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

12.5 Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 12.14.

12.6 The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

12.7 The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC).

12.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:

- physical security controls;

- good industry standard policies and processes;
- malware protection;
- boundary access controls including firewalls;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user access controls, and;
- the creation and retention of audit logs of system, application and security events.

12.9 The contractor shall ensure that any departmental data (including email) 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.

12.10 The contractor shall ensure that any departmental 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 department except where the department has given its prior written consent to an alternative arrangement.

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

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

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

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

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

12.14 In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

12.15 In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

12.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted. In addition, any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

12.17 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.

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

12.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department’s nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

12.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

12.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

12.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.

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

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

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

12.25 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

CALL-OFF SCHEDULE 10 (EXIT MANAGEMENT)

PART A: LONG FORM EXIT MANAGEMENT REQUIREMENTS

1. DEFINITIONS

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

"Exit Information"	has the meaning given to it in Paragraph 3.1 of Part A of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under Part A of this Schedule;
"Registers"	the register and configuration database referred to in Paragraph 2.1 of Part A of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 5.1 of Part A of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of Part A of this Schedule;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Contracts"	has the meaning given to it in Paragraph 8.2.1 of Part A of this Schedule.

2. SUPPLIER MUST ALWAYS BE PREPARED FOR CONTRACT EXIT

2.1 During the Contract Period, the Supplier shall promptly:

2.1.1 create and maintain a detailed register of all Sub-contracts (if any) and other relevant agreements required in connection with the Deliverables; and

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

("**Registers**").

2.2 The Supplier shall procure that all Sub-Contracts (if any) 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.

2.3 Each Party shall appoint an Exit Manager within one (1) Month 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 one (1) Month after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

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

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

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) every [one (1) month] throughout the Contract Period; and

(b) no later than [ten (10) 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 [ten (10) Working Days] following, any material change to the Deliverables (including all changes under the Variation Procedure); and

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

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. TERMINATION ASSISTANCE

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as

reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the date that the Supplier ceases to provide the Deliverables.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than six (6) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.3 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. TERMINATION ASSISTANCE PERIOD

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. OBLIGATIONS WHEN THE CONTRACT IS TERMINATED

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

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

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

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

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

8. ASSETS, SUB-CONTRACTS AND SOFTWARE

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

8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

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

8.2.1 which, if any, of 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 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.

8.4 The Buyer shall:

8.4.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.4.2 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.

8.5 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.

8.6 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 8.3 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 8.6 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 Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

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

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

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

CALL-OFF SCHEDULE 13 (IMPLEMENTATION PLAN AND TESTING)

Part A - Implementation Plan

1. AGREEING THE IMPLEMENTATION PLAN

1.1 The Supplier will provide the Implementation Services in accordance with the Implementation Plan. The Outline Implementation Plan is set out in Annex 1 and the Supplier shall provide the Buyer with a fully developed draft of its detailed Implementation Plan for Approval within ten (10) days of the Call-Off Contract Start Date.

1.2 The draft must contain enough detail for effective management of Contract implementation.

1.3 The Buyer shall not unreasonably withhold Approval of the updated draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it.

2. FOLLOWING THE IMPLEMENTATION PLAN

2.1 The Supplier shall perform its obligations in respect of Delivery and, where relevant, Testing of the Deliverables in accordance with the Approved Implementation Plan.

2.2 The Implementation Plan shall be regularly reviewed and updated, if agreed by both Parties, during Contract Management meetings.

3. DELAYS

3.1 If the Supplier becomes aware that there is, or is likely to be, a Delay it shall;

3.1.1 notify the Buyer in writing within two (2) Working Days of becoming aware, explaining the likely impact of the Delay

3.1.2 use all reasonable endeavours to mitigate the effects of the Delay, including complying with the Buyer's reasonable instructions.

Part B - Testing

1.1 All Tests will be carried out in accordance with the Test Plan.

1.2 The Supplier shall submit the Deliverables in respect of which Tests will be undertaken, as identified in the Test Plan, for the relevant Testing no later than the date specified in the Contract for the Test Period to begin.

1.3 The Supplier shall submit a draft Test Plan for Approval no later than ten (10) days after the Call-Off Start Date.

1.4 The Test Plan will include:

- an overview of how Testing will be carried out
- specific details of each Test to be carried out to demonstrate that the Buyer's requirements are satisfied
- the Test Success Criteria for all Tests
- a timetable for Testing over the Test Period, this to be compliant with any Implementation Plan
- the process for recording the conduct and results of Testing
- the responsibilities of the Parties
- a categorisation scheme for test issues e.g. critical/serious/minor.

1.5 The Buyer shall not unreasonably withhold Approval of the Test Plan provided that the Supplier shall implement the Buyer's reasonable requirements in the Test Plan.

2.1 Unless specified in the Test Plan, the Supplier shall be responsible for carrying out the Testing detailed in the Test Plan.

2.2 The Buyer may require that a Buyer representative witnesses the conduct of the Tests.

2.3 No later than seven (7) days after the completion of the scheduled Test Period the Supplier shall provide the Buyer with a Test Report setting out:

- an overview of Testing carried out
- details of each Test carried out together with the result, indicating if the success criteria were satisfied
- details of any scheduled Tests that were not carried out
- a list of all outstanding Test issues.

3.1 Where by the end of the scheduled Test Period the Testing process has demonstrated that the Test Success Criteria have been met then the Buyer shall notify the Supplier in writing that the Testing process has been satisfactorily completed.

3.2 Where as a result of a Supplier default the Testing process has not by the end of the scheduled Test Period demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer may:

- Direct the Supplier to repeat any unsuccessful Test or undertake any scheduled Test not thus far undertaken to give the Supplier an opportunity to demonstrate that the outstanding issues detailed in the Test Report have been resolved; or

- Notify the Supplier that testing has been satisfactorily completed subject to rectification of outstanding issues within a period specified by the Buyer.

3.3 Where the Supplier fails a second subsequent repeat of the Test then:

- such failure to rectify the relevant issues within the period specified shall be a material Default; or
- the Buyer shall be entitled:

- - to reject the relevant Deliverables and to invoke Clause 3.2.12; or

  - to reject the relevant Deliverables treating this as a material default and invoking the Buyer's termination right under Clause 10.4.1

Annex 1 Outline Implementation Plan

Stage	Dates	Deliverables	Responsibility
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

CALL-OFF SCHEDULE 14 (SERVICE LEVELS)

Definitions

In this Part Call-Off Schedule 14, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

REDACTED	REDACTED
"Performance Monitoring Report"	a Performance Monitoring Report as specified by Section 3 of this Call-Off Schedule 14;
"Service Credits"	any service credits specified in the Annex to Section 2 of this Call-Off Schedule 14 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 Annex to Section 2 of this Call-Off Schedule 14;
"Service Level Failure"	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 Section 2 of this Call-Off Schedule 14; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Section 2 to this Call-Off Schedule 14.

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

1.1 The Supplier shall at all times provide the Deliverables to meet the Service Level Performance Measure for each Service Level.

1.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Section 2 to this Schedule 14 including the right to any Service Credits, which are 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.

1.3 The Supplier shall send Performance Monitoring Reports to the Buyer in accordance with the provisions of Section 3 (Performance Monitoring) of this Call-Off Schedule 14.

1.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where**:**

1.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

(a) the Service Level Failure:

(b) exceeds the relevant Service Level Threshold;

(c) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(d) results in the corruption or loss of any Government Data; and/or

(e) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

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

2. **Critical Service Level Failure**

On the occurrence of a Critical Service Level Failure:

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

2.2 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 Failure") ,

provided that the operation of this paragraph 2 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.

Section 2: Service Levels and Service Credits

1. **Service Levels**

1.1 If the level of performance of the Supplier is likely to or fails to meet any Service Level Performance Measure 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:

1.1.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer;

1.1.2 instruct the Supplier to comply with the Rectification Plan Process;

1.1.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.1.4 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).

1.2 Any failure by the Supplier to achieve a Service Level shall be excused to the extent that such failure results directly from a failure by a Responsible Body or a School to comply with any instruction given by the Buyer in relation to this Call-Off Contract.

2. **Service Credits**

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Section 2 of this Call-Off Schedule 14.

ANNEX

TO SECTION 2: SERVICES LEVELS AND SERVICE CREDITS TABLE

REDACTED

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

REDACTED

Section 3: Performance Monitoring

1. **Performance Monitoring and Performance Review**

1.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of the proposed process for monitoring and reporting of Service Levels, and the Parties will try to agree the process as soon as reasonably possible.

1.2 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") as agreed pursuant to paragraph 1.1 above which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

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

1.2.2 a summary of all failures to achieve Service Levels;

1.2.3 details of any Critical Service Level Failures;

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

1.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

1.2.6 such other details as the Buyer may reasonably require .

1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Monthly basis to review by Performance Monitoring Reports. The Performance Review Meetings shall :

1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued at such location and time (within normal business hours) as the Parties may agree;

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

1.3.3 be fully minuted by the Supplier, with the minutes circulated by to all attendees at the relevant meeting and also any other recipients agreed at the relevant meeting.

1.4 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

CALL-OFF SCHEDULE 15 (CALL-OFF CONTRACT MANAGEMENT)

1. DEFINITIONS

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

Operational Board	the board established in accordance with paragraph 4 of this Schedule;
Project Manager	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. PROJECT MANAGEMENT

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

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

3. ROLE OF THE SUPPLIER CONTRACT MANAGER

3.1 The Supplier's Contract Manager's shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

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

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

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

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

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

4. ROLE OF THE OPERATIONAL BOARD

4.1 The Supplier and the Buyer shall be represented on the Operational Board to be established by the Buyer for the purposes of this Contract.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. CONTRACT RISK MANAGEMENT

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

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

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

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

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Operational Board

- Frequency of the Operational Board to be agreed within ten (10) working days of the Start Date.

- In compliance with Government's COVID-19 distancing rules, Operational Boards shall take place via a Virtual Meeting Platform. The preferred Virtual Meeting Platform will be the one proposed by the Buyer.

- Operational Board must have representatives from the Buyer and the Supplier.

CALL-OFF SCHEDULE 20 (CALL-OFF SPECIFICATION)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyer under this Contract.

Buyer Requirements

The Buyer's plan is that all pupils, in all year groups, will return to school full-time from the beginning of the autumn term. While the Buyer's aim is to have all pupils back at school in the autumn, every school will also need to plan for the possibility of a local lockdown and how they will ensure continuity of education.

In order to support schools and children during these local lockdowns, the Buyer wishes to procure laptops and tablets as part of an initiative to make remote education accessible for pupils who are unable to attend school due to a local lockdown.

The priority in operationalising this service will be getting the support to children who need it in the shortest timeframe. This means prioritising processes that are responsive and using user insights to maximise their effectiveness. This will not be a familiar exercise for all users, and it will be important that the Supplier can provide the technological and ordering support required to enable access.

The requirements detailed below list the minimum specification.

Devices requirements

- The Supplier shall provide and deliver a portable device, which is robust in design and suitable for an educational environment.
- The Supplier will procure a total of 132,500 Devices in the Call-Off Initial Period. The Buyer reserves the right to increase this volume as demand requires.
- Any changes to the Device volumes will be jointly agreed by way of formal variation.
- The Supplier shall provide 132,500 devices; 97,500 Microsoft laptop Devices, 20,000 Google Chromebook Devices and an additional 15,000 tablet Devices with keyboards.
- Annex 1 of this Schedule 20 provides Device specifications and minimum requirements.

Build type and build quantity

- The Supplier must provide all Windows devices with the baseline OEM Windows 10 Pro Education 1909, or newer. Some Devices may have an additional Buyer “Build/configuration” applied per order request, as specified during the ordering process. This will include the option to order an OEM device with or without the supplied image installed.
- The Supplier will ensure all OEM windows Devices will be Windows 10 Pro Education 1909 or newer, without Bloatware,.
- Where the Imaged Device option is selected, the Supplier will provide the chosen Device to order, within the agreed timescales, as specified in Call-Off Schedule 14 (Service Levels).

- The Buyer requires any orders for a Chromebook to capture key information to enable the Device to be enrolled onto a school's existing tenant as a part of the order process.

User Ordering and Support Service

- The Supplier shall provide an online service, to enable ordering of Devices and any agreed ongoing support services. These Devices may be ordered directly by the school, or through the Responsible Body (the organisation that oversees the school, normally an Academy Trust or Local Authority (**LA**)) pending final decision from the Buyer in conjunction with the Supplier.

- The Supplier will provide the Buyer with access to a prototype/staging version of the online service to allow the Buyer to undertake user testing in accordance with the provisions of Schedule 13 (Implementation and Testing).

- The Supplier shall allow amendments to be made to the Services to reflect learning from user research and testing. The Supplier will work through requests for changes.

- The Supplier will provision within or linked to the Services a 'guidance hub' to host information on the Devices, build and policy, accessible without user log-in.

- The Supplier will provide a single point of contact for queries from LAs, Academy Trusts and schools, which will cover all elements of support that might be required through the programme. The Supplier should provide a single, unified service, including for Devices provisioned since May 2020. A handover of the current support service will be provided as necessary. Detailed requirements are outlined in the section below.

- The Supplier will work with the Buyer to maintain a central, shared view of all LA, Academy Trust and school contacts, the queries they have submitted and the communications they have received. The Supplier and the Buyer will send communications to segments of the LAs, Academy Trusts and school contacts depending on factors such as their stage in the ordering and delivery process.

- The Supplier will enable operational communications to be issued to the LA, Academy Trust and school contacts that need to receive them. For example, order confirmations, delivery notifications, dispatch information, etc. The Supplier may also be required to draft these communications adhering to user-centred design principles (including using user insights to inform text).

- The Services will commence from the Call-Off Contract Start Date up to 31 March 2021. Any extensions to the support desk service post 31 March 2021, will be jointly agreed by both parties acting reasonably and in good faith, in line with the extension options detailed in the Call Off Contract, by way of formal variation (as described in Joint Schedule 2).

- The Supplier shall ensure the User Ordering and Support service is available from the Call-Off Contract Start Date as detailed below and as described in Call-Off Schedule 14 (Service Levels):

    - User Ordering and Support Service availability and service levels:

        - Service Hours: Online 24x7 excluding planned maintenance
        - Maintenance support service hours: 8am-5pm, Working Days
        - 99.99% availability SLA

- Out of hours emergency support via supplied call rota with Supplier

- **Minimum Requirements -** The Supplier will provide an ISO/IEC 20001 / ITIL service management troubleshooting and problem resolution service available to the Buyer, schools and Academy Trusts, supporting schools and Academy Trusts to take ownership of the Devices in full before the configured software and safeguarding provision expires, covering:
    - Logistics
    - Delivery
    - Orders
    - Queries related to orders
    - DOA Process
    - Technical queries relating to:
        - local admin
        - password resets
        - device enrolment
        - de-enrolment
        - device resets
    - MDM and filtering solution configuration changes as required by the Buyer
- Single point of contact and triage for technical issues.

Enhanced Support Requirement

The Supplier will provide all Devices with the manufacturer warranty as a minimum.

The Buyer reserves the right to procure an optional extended warranty that can be enacted at any point during the Call-Off Initial Period or Extension Period. This service will utilise the manufacturer warranty procured with the Devices to effect a repair of the Devices for the Buyer at pace.

The Supplier will provide as an optional service for the Buyer, Schools and Academy Trusts with the ability to enact a repair and facilitate the manufacturer warranty for Devices provided under this Call-Off Contract with a Device replacement within one (1) Working Day plus one (1) to ensure Devices are available.

The Supplier will supply and configure a service, working collaboratively with the Buyer to clarify the service design for end users to deliver this extended support provision.

Any extensions to the support service following the Call-Off Initial Period, will be jointly agreed by both parties acting reasonably and in good faith, in line with the extension options detailed in the Call-Off Order Form, by way of formal variation.

The Supplier shall ensure the Enhanced Support Service is available as detailed below and as described in Schedule 14 (Service Levels).

- Enhanced Support Service availability and service levels:

    - Service Hours: Online 24x7 excluding planned maintenance
    - Maintenance support service hours: 9am-5pm, Working Days
    - 99.99% availability SLA
    - Device replacement: one (1) Working Day plus one (1)

The Supplier shall provide access to performance data and reports including the following areas: device ordering, device distribution, service desk/support enquiries handling, portal usage and performance. Data should be near to real time where applicable.

Device Bonded Storage and Insurance

- The Supplier shall procure that bonded storage and appropriate insurances are in place for the Devices procured under this Call-Off Contract and included in Schedule 5 (Pricing).

- The Supplier will store the Devices in a secure location until order fulfilment is complete.

Storage requirements:

- During the Call-Off Initial Period any remaining Devices shall be distributed by the Supplier in accordance with the Buyer's reasonable instructions
- In the event the Buyer exercises the extension options as described in the Call-Off Order Form the following additional storage requirements may be required;
  - From 1 April 2021 until 30 September 2021 and then any remaining Devices shall be distributed by the Supplier in accordance with the Buyer's reasonable instructions
  - From 1 October 2021 until 31 March 2022 and then any remaining Devices shall be distributed by the Supplier in accordance with the Buyer's reasonable instructions

Delivery

- The Supplier will deliver the specified Devices to the agreed locations during the next Working Day if the order is placed before 4pm or if the order is placed after 4pm, during the second Working Day following the order, as described in Schedule 14 (Service Levels). Schools may select a specific delivery date which will take precedence over the 24-hour SLA. Delivery of the Devices shall be made between the hours of 8.00am and 6.00pm on a Working Day.

- The Supplier shall provide a facility for a Responsible Body/school to return Devices if incorrectly ordered.

High Level Service Design and Service Levels

A service design with agreed service levels will be developed and agreed by the Supplier and the Buyer in the Co-design Process that will establish expectations and responsibilities of both Parties; that will provide a quality service that is easy to monitor. Key phases including:

- Phase 1 - ordering the required hardware and inbound logistics of the same
- Phase 2 - setting up the processes and online service enabling orders to be placed in the event of local lock-down(s)
- Phase 3 - executing the ordering process as agreed by the Parties in line with Government advice and prioritisation on local lockdowns; enabling eligible schools/RBs to order up to a pre-agreed cap
- Phase 4 - fulfilment / delivery of 90% within one (1) Working Day on order (assuming order before 4pm) of requirement Device types within the eligibility criteria agreed by the Buyer
- Phase 5 - Logistics on distributing remaining Devices in line with Buyer requirements / mop-up and decommissioning.

During the Contract Term, the Supplier shall provide service support on each phase, for example, assisting with communications.

Indicative Service Levels may include:

- User Ordering and Support Service 24/7 Excluding planned maintenance

- Supplier Team available to answer inbound enquiries around Dead on Arrival (DOA) equipment and user ordering service enquires between the hours of Monday – Friday, 0900

-1700 on Working Days

- When a school/RB is confirmed as being in a local lockdown, they are able to place an order on the User Ordering Service within two hours of the Supplier being notified by the Buyer (Monday to Sunday 8am to 6pm)

- Upon receipt of an order by the RB/School via the User Ordering Service, despatch of the order by the Supplier will be completed within one (1) Working Day in 90% of orders and two (2) Working Days for 100%.

- The Supplier will deliver the specified Devices to the agreed locations during the next Working Day if the order is placed before 4pm or if the order is placed after 4pm, during the second Working Day following the order.

- The Supplier shall within one (1) Working Day of receipt of new stock of each part number supply two sample machines to the Buyer for the purposes of the Buyer testing images.

Annex 1 - Device Specifications

All Devices should be current specifications available to retailers, not out of commission specifications.

Microsoft Laptop/Tablet Devices

The Device shall be:

- Usable for continuous periods of time (minimum morning or afternoon session) without re-charging (target 7 hours)
- Able to support dual monitor display, i.e. simultaneous display to internal monitor and external monitor/AV
- High definition resolution at a minimum
- Capable of simultaneous moderate-intensity tasks and running the standard/curricular software provided
- Capable of capturing visual and audio content using inbuilt facilities
- Configured with a single image that can be used securely and safely 'out of the box' where required
- All Devices provided must have integrated, non-detachable batteries

The Device shall conform to the following minimum specifications:

- 11" screen (10" minimum for Tablet form factor)
- 4Gb RAM
- 64Gb SSD HDD
- Webcam
- Headphone/microphone socket
- Wifi to 802.11ac
- Speaker
- 2 x USB 3.0 Type A socket (1 x USB 3.0 Type C would be desirable instead of a Type A socket) - At least one USB Type A socket to support charging/powering of peripherals/devices
- UK Standard Keyboard; require attachable/detachable keyboard for tablets
- Minimum 1-year warranty return to base, 48-hour turnaround
- Sleeve case
- Windows 10 Professional Education / Shape the Future. Minimum version of 1909. S-mode not enabled. Operating system license included. License required for standalone use and subsequent connection of the Device to a school network/domain. Windows licences must be preactivated and valid on main and recovery partitions on shipment from manufacturer
- No Bloatware on main or recovery partitions – Desirable requirement
- Video port
- PSU fitted with UK 3-pin as standard
- Security features – confirm TPM2 minimum requirement
- Software image consistency 12 month minimum
- SCCM support driver pack must be available
- Autopilot enabled with PKID/hardware# - please confirm and where located
- EUFI and evergreen commitment. Remote management desirable.
- Compliancy – energy star certified

Chromebook Mobile Device (cloud-enabled computing device)

The mobile Device with local processing power for accessing cloud-based applications and resources.

- The Device must be capable of being used for a continuous period of time (minimum morning or afternoon School session, ideally all day) without the need to re-charge the battery. (target 10 hours)
- The Device must be robust in design and suitable for an educational environment.

The Device shall conform to the following minimum Specifications:

- 11” screen minimum
- 4gb ram
- 16gb SSD HDD minimum
- Wifi to 802.11ac
- Speaker
- 1 x USB 3.0 Type A socket and 1 x USB 3.0 Type C socket
- Keyboard
- HD Webcam
- Headphone/microphone socket
- Minimum 1-year warranty return to base, 48-hour turnaround
- Sleeve case
- Device management license for remote cloud administration shall be included
- PSU fitted with UK 3-pin as standard
- HD minimum screen resolution
- Compliancy energy star certified

A breakdown of the minimum specification requirements for each device type can be found in the below file. As part of the tender activity, suppliers will complete this template providing specification details of their proposed device models:

Devices Minimum Specification Templat

Annex A Device Specification

REDACTED

CALL-OFF SCHEDULE 4 (CALL-OFF TENDER)

Annex A – Quality Response

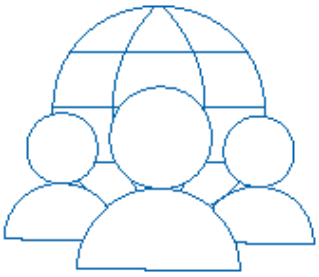
REDACTED

Annex B – Pricing Response

REDACTED

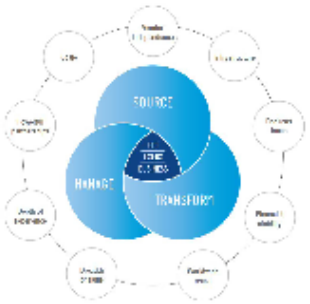
Annex C – Modern Slavery Statement

MODERN SLAVERY STATEMENT 2019



At Computacenter, we continue to observe high ethical standards in the conduct of our business activities and within our supply chain. We are dedicated to responsible and sustainable corporate management. This includes making sure that the group's practices are compliant with human rights and employment legislation wherever we do business.
We are a leading independent technology partner trusted by large corporate and public sector organisations. We Source, Transform and Manage technology for our customers in 70 countries worldwide.

Our business is diversified across our main territories and our three business areas, which are described below. These businesses are distinct, but synergistic, as customers increasingly look to buy end-to-end services and solutions, ranging from consulting to integration over the product's supply life cycle, to contracting a managed service.



Our Ambition:

- Strongly recommended by customers for the way we help them achieve their goals;
- The preferred route to market for technology providers;
- People want to join us and stay with us, proud of our reputation, as we learn, earn and have fun;
- Trusted as an agile & innovative provider of digital technology around the world.

Who we are:
Computacenter is a leading independent technology partner trusted by large corporate and public sector organisations.

What we do:
We help our customers to source, transform and manage their technology infrastructure to deliver digital transformation, enabling users & their business.

Our footprint matches where our customers are headquartered and global reach to support their worldwide service requirements. Computacenter is headquartered in the UK.
Within the Computacenter group, we have over 17,000 people based across Europe, America, Mexico, South Africa and Asia Pacific
We have developed a global coverage to mirror our customer's requirements. As a result, we sell to customers in nine countries: UK, Ireland, Germany, France, Belgium, Switzerland, the Netherlands, USA and Spain.

We also have operations/entities in another 12 countries: Hungary, Poland, India, Mexico, China, Malaysia, Japan, Australia, Hong Kong, Singapore and Canada and South Africa.

We source for and support customers in another 49 countries.

Our extensive partner network covers field services and onsite support and globally services Computacenter's European headquartered customers.
Our supply chain is made up of products and services that we use in our business; our employees and contractors; partner organisations who we work with; and IT equipment which we supply to our customers.
As signatories to the United Nations Global Compact, we are committed to upholding internationally proclaimed human rights. For Computacenter, human rights fall into two areas: protecting the rights of our employees and ensuring we are not complicit in human rights abuses in our supply chain.

The human rights of our employees are covered by our people policies and compliance with local labour laws wherever we do business.

Annex D – SFIA Rate Card

REDACTED