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

Order Form

CALL-OFF REFERENCE:	project_4892
THE BUYER:	The Secretary of State for Education
BUYER ADDRESS:	20 Great Smith St, Westminster, London SW1P 3BT
THE SUPPLIER:	Computacenter UK Ltd
SUPPLIER ADDRESS:	Hatfield Ave, Hatfield, Hertfordshire 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 11th of November 2020.
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):

- 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:

This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

1. Joint Schedule 1(Definitions and Interpretation) RM6068
2. The following Schedules in equal order of precedence:
   - Joint Schedules for RM6068
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)

    - Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 11 (Processing Data)
- Call-Off Schedules for project_4892
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 9 (Security)
    - Call-Off Schedule 13 (Implementation Plan and Testing)
    - Call-Off Schedule 14 (Service Levels)
    - Call-Off Schedule 20 (Call-Off Specification)

3. CCS Core Terms (version 3.0.6)
4. Joint Schedule 5 (Corporate Social Responsibility) RM6068
5. 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.
6. Annexes A to E Call-Off Schedule 6 (ICT Services)

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
None

CALL-OFF START DATE: **11/11/2020**

CALL-OFF EXPIRY DATE: **10/11/2021**

CALL-OFF INITIAL PERIOD: 1 Year

CALL-OFF OPTIONAL EXTENSION: N/A
PERIOD

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

LOCATION FOR DELIVERY
The Supplier will deliver the hardware units to Hatfield Avenue, Hatfield AL10 9TW.

DATES FOR DELIVERY OF THE DELIVERABLES
See details in Call-Off Schedule 13 (Implementation Plan & Testing)

TESTING OF DELIVERABLES
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.

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

Each Party's total aggregate liability under this Call-Off Contract (whether in tort, contract or otherwise) is 125% of the Contract Value.

CALL-OFF CHARGES
Initial Order Value £86,960,890.06
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:
Department for Education
Sanctuary Buildings
20 Great Smith Street
London
SW1P 3BT

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)
Not Applicable

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:	**project_4892 ("the Contract")**	
Contract reference number:	**project_4892**	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

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

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

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

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need to have

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

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

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

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

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

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

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

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

2. How to manage the insurance

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

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

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

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

3. What happens if you aren't insured

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

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

4. Evidence of insurance you must provide

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

5. Making sure you are insured to the required amount

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

6. Cancelled Insurance

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

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

7. Insurance claims

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

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

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

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

ANNEX: REQUIRED INSURANCES

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

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

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

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

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

Joint Schedule 4 (Commercially Sensitive Information)

2. What is the Commercially Sensitive Information?

2.1 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.

2.2 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).

2.3 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
	REDACTED	REDACTED	REDACTED
		REDACTED	
		REDACTED	
		REDACTED	
		REDACTED	
		REDACTED	

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:

4.1a 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 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;

5.4 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:

5.4.1 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;

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

5.4.3 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

5.4.4 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

5.5 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:

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

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

25.3 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

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

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

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

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

Annex 1 - Processing Personal Data

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

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

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

Personal Data Processing

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: REDACTED
Duration of the Processing	REDACTED
Nature and purposes of the Processing	REDACTED
Type of Personal Data	REDACTED
Categories of Data Subject	REDACTED

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	REDACTED

Call-Off Schedule 1 (Transparency Reports)

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

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within five (5) working 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) working days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

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

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
REDACTED	• REDACTED	REDACTED	REDACTED
REDACTED	• REDACTED	REDACTED	REDACTED
REDACTED	• REDACTED	REDACTED	REDACTED
REDACTED	• REDACTED	REDACTED	REDACTED
REDACTED	• REDACTED	REDACTED	REDACTED

Call-Off Schedule 5 (Pricing Details)

Call-Off Schedule 5

Pricing Details

1. Charges

1.1 The price for the hardware units, detailed in Annex A below, is:

The Supplier has submitted the following Pricing Schedule as part of the ITT response:

REDACTED

From the above Pricing Schedule, the Buyer has selected the following as final split that will form the contract.

REDACTED

Initial Order Value is £86,960,890.06.

The Buyer has not committed to any volumes for Android Tablets, however it reserves the right to purchase up to 50,000 if required during the life of the contract. This totals an uncommitted spend of up to REDACTED. Purchase of any Androids Tablets will require the implementation of a separate Variation Form as per Joint Schedule 2.

For any potential future purchases and / or variations under this contract, rates from the ITT Pricing Schedule will apply. However please see below due to market fluctuations:

REDACTED

2. INVOICING

2.1 The Supplier will invoice the Buyer for hardware units at the point at which units are received at the nominated point of delivery and evidence of such arrival has been duly supplied and verified by the Buyer.

2.3 Invoices are payable on 30 days terms from receipt of the invoice.

3. ASSUMPTIONS

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

REFERENCE		Assumptions
A-001	REDACTED	REDACTED
A-002	REDACTED	REDACTED
A-003	REDACTED	REDACTED

A-004	REDACTED	REDACTED
A-005	REDACTED	REDACTED
A-006	REDACTED	REDACTED

3.2 In the event that any one or more of the Assumptions set out in paragraph 3.1 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:

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

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

Annex A – OEM Warranty Turnaround Time

REDACTED

Call-Off Schedule 6 (ICT Services)

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

ANNEX B

COTS Licensing Terms

Third party software (if any) shall be licensed subject to the third party licensor's standard license terms attached which shall govern the supply, the Buyer'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

N/A

Annex E

Device as a Service Terms

N/A

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:
   - the Departmental Security Requirements (Annex 1)
   - 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
   - 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
   - the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
   - 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
   - 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"	means the Security and Information Risk Advisor (SIRA) is a role defined under the

"SIRA"	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

1.1. 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.

1.2. 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).

1.4 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).

1.5 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.

1.6 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.

1.7 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).

1.8 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.

1.9 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.

1.10 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.

1.11 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.

1.12 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".

1.13 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.

1.14 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.

1.15 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.

1.16 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.

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

1.18 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.

1.19 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.

1.20 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.

1.21 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.

1.22 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.

1.23 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.

1.24 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.

1.25 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 13 (Implementation Plan and Testing)

Part A – Implementation Plan

1. Agreeing the Implementation Plan

1.1 The Supplier's tendered draft Implementation Plan is at Annex 1 to this Part A of Call-Off Schedule 13. The Supplier will provide an updated, fully developed draft for Approval within 5 days of the Call-Off Contract Start Date.

1.2 The updated 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 Changes to any Milestones, Milestone Dates, Milestone Payments or Delay Payments shall only be made via the Variation Procedure.

2.3 Where the Supplier is responsible for the failure to achieve a Milestone by the date specified in the Approved Implementation Plan this shall constitute a material Default.

3. Delays

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

- Notify the Buyer in writing within 2 Working Days of becoming aware, explaining the likely impact of the Delay

- Use all reasonable endeavours to mitigate the effects of the Delay, including complying with the Buyer's reasonable instructions

Annex 1 Draft Implementation Plan

As part of the ITT, the Supplier provided the below delivery Schedule:

REDACTED

From the above schedule, the Supplier will deliver to the following total number of devices:

- **REDACTED**Android Tablets: 0 committed, opportunity to purchase up to 50,000 if required

The Agreed Delivery Schedule based on the selected Devices is the following:

REDACTED

Delivery timelines are crucial to reducing the time children in England may be unable to access remote education. As such, we require devices delivered under this contract to arrive in regular and steady flow as soon as possible after they are manufactured, with the final shipments to be delivered by 7th February 2020.

Where Devices ordered are more than 14 days later than the dates stated in the agreed Delivery Schedule, the Buyer has the right at their discretion to reject delivery, refuse payment and cancel that part of the order for any late items at no cost to the Buyer.

Part B – Testing

In this Part B to Call-Off Schedule 13, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"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 this Part B to Call-Off Schedule 13;

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

1.2 The Supplier shall submit each Deliverable for the relevant Testing no later than the date specified in the Contract for the Test Period to begin.

2.1 The Supplier shall submit a draft Test Plan for Approval no later than 5 days after the Start Date.

2.2 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 eg critical/serious/minor

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

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

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

3.3 No later than 5 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

4.1 Where by the end of the scheduled Test Period the Testing process has demonstrated to the Buyer's satisfaction 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.

4.2 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. Failure to rectify the relevant issues within the period specified shall be a material Default; or

- 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

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):

"**Critical Service Failure"**	Means a failure to meet a Service Level Threshold in respect of a Service Level
Performance Monitoring Report	Means a Performance Monitoring Report as specified by Section 3 of this Call-Off Schedule 14
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to 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

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

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

3.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Section 2 to this Schedule 14.

3.3 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.

4. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

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

provided that the operation of this paragraph 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.

4.2 Where Devices ordered are more than 14 days later than the dates stated in the Agreed Delivery Schedule, the Buyer has the right at their discretion to reject delivery, refuse payment and cancel that part of the order for any late items at no cost to the Buyer.

Section 2: Service Levels

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;

and/or

1.1.3 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).

Annex 1 to Section 2: Services Levels and Service Credits Table

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure
REDACTED	REDACTED	REDACTED

Section 3: Performance Monitoring

5. 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 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.

Call-Off Schedule 20 (Call-Off Specification)

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

Specification

The supplier will be required to provide up to 460,000 laptop or tablet devices to form part of DfE's Get Help With Technology – Devices Reserve Programme. The exact amount purchased will be agreed at the contracting stage and may be any amount up to 460,000. The figure of 460,000 will be used for price evaluation purposes, however the Buyer reserves the right to order any amount of devices up to the total 460,000 devices and amend the mix of device types and models as is required when contracting. The unit prices you submit will apply regardless of the final number and mix of devices purchased. The Department may also amend the total of 460,000 through clarification questions prior to the clarification deadline depending on the outcome of a current procurement to purchase supplier's existing stock.

The Department is also exploring a potential requirement for Android tablets with its end users. As such, suppliers are required to provide a price and delivery dates for these devices. This will not be scored however may be taken up as an option during the contract term and suppliers will be held to the unit price provided.

The total number of devices will be made up of multiple device types, with the below estimates provided to give indicative figures (however, as above the final mix of device types can be amended to any mix within the total amount purchased):

Chromebooks: 150,000

Apple Tablets: 50,000

Windows Laptops: 210,000

Windows Tablets: 50,000

Android Tablets: 50,000 **(NON-SCORED OPTION)**

While price plays an important factor, the department will look to derive the long-term value of remote education and technology in the classroom through these devices. Devices should present a sound long term investment and be robust enough to give value for several years in an education setting.

What is paramount, is short delivery timelines which are crucial to reducing the time children in England may be unable to access remote education. As such, we require devices delivered under this contract to arrive in regular and steady flow as soon as possible after they are manufactured, with the final shipments to be delivered by 7th February. Our ideal scenario is regular and significant volumes from November / December 2020 and throughput January 2021 to ensure delivery, inbound logistics and onward dispatch to Trusts and Schools is not constrained.

It will be critical that the delivery happens in the shortest time possible. The Department will work with the successful supplier to ensure OEM manufacturer timelines and the impact on deliverability for the service to expedite deployment as soon as we are notified of a school closure. This is entirely dependent on the amount of available stock in the reserve. Some devices will be built with an additional Departmental “Build/configuration” applied per order request, on top of the Windows 10 Professional Education 1909 or newer operating system. Our preferred operating system is Windows 10 Professional Education 2004.

We will look to deploy devices in a short timeframe and will look to prospective suppliers to advise on how quickly they could provide devices into England to support the Service. Deployment is currently reactive but should move to proactive as inbound stock arrives. While we are currently operating a model in which the school (or the Trust that oversees it) notifies our services supplier that they require devices and the number of devices that they need through an online user ordering and support system that the supplier operates. This is validated by the Department and the order should be progressed the same day. Stock permitting, we will look to transition to a proactive ordering approach deploying devices ahead of a school closure or order system. Devices will, for the most part, be delivered directly to the schools although may be ordered by the Trust or Local Authority that oversees the school. We are finalising the eligibility criteria for the devices.

This is a complex delivery project with a requirement for devices being manufactured, shipped, built and deployed. There will be a large number of moving parts. We will expect the successful supplier to set out a clear daily reporting process for the movement of devices to England, inbound logistic inclusive of pre-manufacture, manufacture, provisional delivery dates, confirmed delivery dates, actual delivery dates to support planning and deployment progress across England.

We expect the successful supplier to:

- hold the delivered stock in a secure UK location until requested by the Authority or the Authority’s Services partner. This stock will need to be transferred in small quantities to the Authority’s Services Partner location(s) as instructed by the Authority
- provide a Dead on Arrival (DOA) process and cover all operating costs of the DOA process as undertaken between the Schools and the Authority’s Services partner
- supply of devices in advance of the main units for testing and build sign off by the Authority and the Authority’s Service Partner
- support the Authority on any and all technical / performance issues discovered with any supplied devices
- work to industry standard booking in processes as set out by the Authority's services provider
- be wholly responsible for stock management and the provision of required booking-in information to the Authority and the Authority's services provider prior to delivery to the Authority's distribution / services providers location
- provide the Authority and the Authority’s services provider with daily inbound stock reporting in an agreed format between the parties

Unit price of the devices will include bonded storage between the date of arrival until the 31st of March 2021 unless otherwise agreed to this Contract though a CCN.

The supplier must commit to a specification on order.

The Buyer is required to agree changes to device specifications 10 days prior to the change being made (with exceptions at the Buyer's discretion).

Device specifications must be submitted to the Buyer for review and acceptance 10 days prior to a production run.

Device Specifications – Minimum Requirement set out in Official Tender

All devices should be current specifications available to the education market, not out of commission or end of life specifications.

Unit price per model proposed must include bonded storage and delivery e.g. supplier will bear the cost of bonded storage and delivery as part of the unit price put forward.

All devices must come individually packaged, with device serial numbers on the outside of the box.

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 (720x1280 or better)
- 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)
- Dual core CPU minimum (Laptop) / Dual Core CPU minimum (Tablet)
    - PassMark CPU benchmark of 2,200 preferred (https://www.cpubenchmark.net/)
    - Must be current generation processor
- 4Gb RAM
- 64Gb SSD

- Webcam VGA (480p minimum), 720p or greater preferred
- Headphone/microphone socket
- Wifi to 802.11ac minimum
- Internal Speaker(s)
- 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
- Hardware hash supplied in Intune compatible CSV format preferred, where not possible details of mechanism that can be used by schools to generate this hash on receipt of devices should be suppled.
- Minimum 1-year warranty return to base – manufacturer turnaround time to be outlined in the Price Schedule document
- Sleeve case
- Windows 10 Professional Education version 1909 or 2004 (2004 Preferred). 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 pre-activated with a UEM key embedded in the UEFI and valid on main and recovery partitions on shipment from manufacturer
- Recovery partition must be present on the devices
- 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
- BIOS: UEFI and evergreen commitment, Network boot (PXE) and 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.

- It 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 (720p or greater)
- Headphone/microphone socket
- Minimum 1-year warranty return to base – manufacturer turnaround time to be outlined in the Price Schedule document
- Sleeve case
- Device management license for remote cloud administration shall be included
- PSU fitted with UK 3-pin as standard
- HD minimum screen resolution (720 x 1080 minimum)
- Compliancy energy star certified
- Google for Education licences must be included in the unit price submitted

Apple iPad

- The device shall meet the following minimum specification:
- Apple 10.2-inch iPad Wi-Fi 32GB (7th Generation Minimum, 8th Generation Preferred)
- Sleeve case

Android Tablets (non-scored option)

The device shall be:

- Usable for continuous periods of time (minimum morning or afternoon session) without re-charging (target 7 hours)
- High definition resolution at a minimum (720x1280 or better)
- Capable of simultaneous moderate-intensity tasks and running the standard/curricular software necessary to delivery remote education
- Capable of capturing visual and audio content using inbuilt facilities
- All devices provided must have integrated, non-detachable batteries

The device shall conform to the following minimum specifications:

- 10” minimum
- Dual Core CPU minimum
- 2Gb RAM
- 32GB RAM minimum, 64 GB preferred and with a preference for SD/Micro SD expandable capability
- Front and Rear facing cameras 2.1mp min – 6mp preferred – capable of 720p video resolution or better (front facing camera) usable in supplied sleeve/case
- Headphone/microphone socket
- Wifi to 802.11ac minimum
- Bluetooth
- Internal Speaker(s)
- 1 x USB 2.0 Type A socket (1 x USB 3.0 Type C would be desirable instead of a Type A socket)UK Standard on-screen Keyboard; require attachable/detachable/ Bluetooth connected keyboard for tablets to be provided as an option, pricing to be provided separately, e.g. tablet and tablet w/keyboard
- Minimum 1-year warranty return to base – manufacturer turnaround time to be outlined in the Price Schedule document

- Current Android Operating system with guaranteed android version updates and security updates for next 3 years
- PSU fitted with UK 3-pin as standard

Annex A: Device Specifications – Devices supplied by Supplier

REDACTED

REDACTED

REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED

REDACTED