

## Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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

## Order Form

CALL-OFF REFERENCE:	<b>con_7218</b>
THE BUYER:	The Secretary of State for the Department for Education
BUYER ADDRESS	20 Great Smith St, Westminster, London SW1P 3BT
THE SUPPLIER:	XMA LTD
SUPPLIER ADDRESS:	UNIT 44 WILFORD INDUSTRIAL ESTATE RUDDINGTON LANE WILFORD NOTTINGHAM NG11 7EP
REGISTRATION NUMBER:	2051703
DUNS NUMBER:	<b>29-848-4148</b>
SID4GOV ID:	<b>NOT APPLICABLE</b>

### APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 20/1/2021. 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:

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

Call-Off Schedule 13

Project Version: 2

RM6068

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

2. Joint Schedule 1 (Definitions and Interpretation) RM6068
3. 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 con\_7218
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 9 (Security)
    - Call-Off Schedule 13 (Implementation Plan and Testing)
    - 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)

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

Without prejudice to other remedies available in the Contract; where it is indicated that Devices ordered are forecasted to be delivered later than 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.

CALL-OFF START DATE: 20/1/2021

CALL-OFF EXPIRY DATE: 19/01/2022

CALL-OFF INITIAL PERIOD: **12 months**

CALL-OFF OPTIONAL EXTENSION PERIOD **N/A**

#### CALL-OFF DELIVERABLES

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

#### LOCATION FOR DELIVERY

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

The Supplier will deliver the hardware units to Delivery location: Computacenter, Hatfield Warehouse.

Title to Goods is transferred to the Buyer on payment to the Supplier in full (save in respect of software where title to the same shall remain at all times with the relevant licensor).

#### **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**

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

Call-Off Schedule 13

Project Version: 2

RM6068

**Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

20 Great Smith Street  
London  
SW1P 3BT

BUYER'S AUTHORISED REPRESENTATIVE  
**REDACTED**

BUYER'S ENVIRONMENTAL POLICY  
N/A

BUYER'S SECURITY POLICY  
See Call-Off Schedule 9 (Security).

SUPPLIER'S AUTHORISED REPRESENTATIVE  
**REDACTED**

SUPPLIER'S CONTRACT MANAGER  
**REDACTED**

**PROGRESS REPORT FREQUENCY**

Daily inbound stock position report to be provided to the DfE. DfE will provide template and data fields required within 5 days of contract signature, agreed between parties. Daily inbound stock reports submitted must come with commentary as to what has changed, either earlier or later per device type, and why.

Report to be provided to the following Buyer Representatives:  
**REDACTED**

**PROGRESS MEETING FREQUENCY**

Weekly progress meetings.

More frequent sessions may be required for specific operational handovers between DfE and Supplier as appropriate and to be defined and agreed by the parties.

**KEY STAFF**

Not Applicable

**KEY SUBCONTRACTOR(S)**

Not Applicable

**COMMERCIALLY SENSITIVE INFORMATION**

Call-Off Schedule 13

Project Version: 2

RM6068

**Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

See Joint Schedule 4 (Commercially Sensitive Information).

SERVICE CREDITS

N/A

ADDITIONAL INSURANCES

N/A

GUARANTEE

N/A

SOCIAL VALUE COMMITMENT

N/A

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

**REDACTED**

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

**REDACTED**

## Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

# 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
No.	Date	Item(s)	Duration of Confidentiality
1	Commencement Date	Pricing	Duration of the contract
2	Commencement Date	Processes including sensitive supply chain agreements	Duration of the contract
3	Commencement Date	Sensitive Personnel details	Duration of the contract

## **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

# **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

Call-Off Schedule 13

Project Version: 2

RM6068

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- 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;



### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 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;

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 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

Call-Off Schedule 13

Project Version: 2

RM6068

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

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

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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*).

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

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 paragraphs 16 to 27 of this Joint Schedule 11.

## Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

### 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	<p><b>The Parties are Independent Controllers of Personal Data</b></p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"><li>• Business contact details of Supplier Personnel for which the Supplier is the Controller,</li><li>• 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.</li><li>• Home address details of DfE employees, required for Supplier to ship test devices to.</li></ul>
Duration of the Processing	<p>Each party will process the personal data only for as long as is necessary in order for them to meet their obligations under the contract for a period not exceeding 6 years after the expiry of the contract.</p>

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

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. in order to meet the requirements of the contract.
Type of Personal Data	Business contact details of Supplier Personnel; directors, officers, employees, agents, consultants and contractors of Relevant Authority.
Categories of Data Subject	Staff (including contractors, volunteers, agents, and temporary workers).
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	Each party will ensure secure destruction of the data after a period not exceeding 6 years following the expiry of the contract.

## **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

## **Call-Off Schedule 5 (Pricing Details)**

**Call-Off Contract charges: £5,725,971.53**

**Breakdown of Call-Off Contract charges:**

**REDACTED**

**Additional information:**

- Prices are inclusive of delivery to the delivery location selected.
- Prices exclusive of VAT.

## **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):



### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

[“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.

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

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**

Call-Off Schedule 13

Project Version: 2

RM6068

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

<p>“BPSS”</p> <p>“Baseline Personnel Security Standard”</p>	<p>means the Government’s HMG Baseline Personal Security Standard . Further information can be found at:</p> <p><a href="https://www.gov.uk/government/publications/government-baseline-personnel-security-standard">https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</a></p>
<p>“CCSC”</p> <p>“Certified Cyber Security Consultancy”</p>	<p>is the National Cyber Security Centre’s (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards.</p> <p>See website:</p> <p><a href="https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy">https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy</a></p>
<p>“CCP”</p> <p>“Certified Professional”</p>	<p>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:</p> <p><a href="https://www.ncsc.gov.uk/information/about-certified-professional-scheme">https://www.ncsc.gov.uk/information/about-certified-professional-scheme</a></p>
<p>“CPA”</p> <p>“Commercial Product Assurance”</p> <p>[formerly called “CESG Product Assurance”]</p>	<p>is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website:</p> <p><a href="https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa">https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa</a></p>
<p>“Cyber Essentials”</p> <p>“Cyber Essentials Plus”</p>	<p>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.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers:</p> <p><a href="https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body">https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body</a></p>

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

"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.

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

“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: <a href="https://www.gov.uk/government/publications/government-security-classifications">https://www.gov.uk/government/publications/government-security-classifications</a>
“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.

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

"NCSC"	The National Cyber Security Centre (NCSC) is the UK government's National Technical Authority for Information Assurance. The NCSC website is <a href="https://www.ncsc.gov.uk">https://www.ncsc.gov.uk</a>
"OFFICIAL" "OFFICIAL-SENSITIVE"	<p>the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP).</p> <p>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.</p>
"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"	<p>means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.</p> <p>NCSC Guidance can be found at: <a href="https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media">https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</a></p> <p>The disposal of physical documents and hardcopy materials advice can be found at: <a href="https://www.cpni.gov.uk/secure-destruction">https://www.cpni.gov.uk/secure-destruction</a></p>
"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:

### Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

	<a href="https://www.ncsc.gov.uk/articles/about-certified-professional-scheme">https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</a>
“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. <a href="https://www.gov.uk/government/publications/security-policy-framework">https://www.gov.uk/government/publications/security-policy-framework</a>

- 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

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).



### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 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.

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 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.

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 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.

### **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

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.

## **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 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 13 (Implementation Plan and Testing)**

### **Part A – Implementation Plan**

#### **1. Agreeing the Implementation Plan**

Call-Off Schedule 13

Project Version: 2

RM6068

## **Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

- 1.1 The Supplier's tendered draft Implementation Plan is at Annex 1 to this Part A of Call-Off Schedule 13. The Supplier guarantees that the delivery schedule submitted is accurate and will be met.

### **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.
- 2.4 Where the Supplier does not meet the latest delivery date of 7th February 2021, this shall constitute a material Default that will allow the Buyer to cancel all or part of the order at the Buyer's discretion.

### **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 1 Working Day 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

**Call-Off Schedule 13: (Implementation Plan and Testing)**

Call-Off Ref:

Crown Copyright 2018

**Annex 1 - Implementation Plan**

The Supplier guarantees to the DfE that it will meet the Delivery Schedule below.

Where the Supplier does not meet the latest delivery date of 7<sup>th</sup> February 2021, this shall constitute a material Default.

**REDACTED**

## 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):

<b>"Test Plan"</b>	a plan for the Testing of the Deliverables to demonstrate compliance with Contract requirements;
<b>"Test Report"</b>	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 1 day 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 1 day 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

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

Crown Copyright 2018

### **Device/Build Validation**

The DfE may require testing of devices, this will be agreed upon contract signature. Where testing is required, the DfE will require:

- Provision of Test Units to DfE: 3 evaluation units per each device model variant. Individuals and their addresses to which test kit is sent will be agreed between the parties separately.
- Provision of Test Units to Service Provider: 3 evaluation units per each device model variant. The devices should be sent to:
  - o Nominated address of Service Provider

Tracking information and confirmation of when the evaluation units will be delivered should be shared with the DfE.

The DfE reserves the right to approve or reject the devices from a quality perspective in the event that these don't meet the required performance expectations.

### **Delivery Information**

The below information outlines the details for the full delivery schedule of all devices.

Required delivery of the Goods to the Delivery Location to be organised by the Supplier.

Delivery location: Nominated address of Service Provider

### **Testing Schedule**

Framework Ref: RM6068  
Project Version: v0.1  
Model Version: v3.2

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

Crown Copyright 2018

The DfE will perform tests on each make/model of the devices received as part of the Device/Build Validation activity.

The DfE will test the devices and confirm whether the devices will be able to perform correctly in line with the minimum DfE performance and quality standards. DfE will be testing functionality to work with our builds and meets the minimum specification to deliver remote education.

The DfE reserves the right to accept or reject the devices based on whether these meet the minimum specification to be delivered to disadvantaged children for the purposes of remote education.

The DfE will provide confirmation / rejection via electronic mail to the selected Supplier representative.

In specific, the testing of each device will look to verify the following features, including but not limited to:

- Performance test of video call, simulating a remote learning environment
- Browser performance
- Call / video clarity using inbuilt camera, microphone and speakers and using headphone/microphone socket(s)
- Bulk build bench-run with DfE build in combination with DfE and DfE's services supplier
- Windows licencing and activation checks
- BIOS password process can be automated / scripted or run manually at scale, meeting the minimum security requirement for password strength
- Units need to arrive packaged in their own individual box, not in batches within the same box
- Hardware hash and serial number available on the box / in the BIOS

For any new model provided, test scripts to be agreed between buyer and supplier with 5 days of contract signature.



## **Call-Off Schedule 20 (Specification)**

### **RM6068 Get Help With Technology – Wave 6 Spot Buy Specification**

The DfE requires in-stock or already in the process of being manufactured Devices and sleeves. The devices required by the DfE are the following:

- Microsoft Laptops
- Microsoft Tablets
- Apple iPads
- Google Chromebooks inclusive of Google Chrome Education Upgrade licenses
- Android Tablets

The DfE has no preferred split between the devices outlined above.

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 (A total of 6 test units per model, if requested by the Buyer)
- 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 and warehousing between the date of arrival until the 31st of March 2021 unless otherwise agreed to this Contract through a CCN. Unit prices must also include the DOA replacement at 1% per model of the order volume.

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.

## Annex A – Windows Laptop Specifications

Device Requirement - Minimum Specification	Laptop Model 1	Laptop Model 2	Laptop Model 3	Laptop Model 4
Make / Model (SKU)	Dell Latitude 3190	GeoBook 2e (GE126)	GeoBook 2e (GE127)	GeoBook 2e (GE175)
<ul style="list-style-type: none"> <li>Usable for continuous periods of time (minimum morning or afternoon session) without re-charging (minimum 7 hours, 10 hour target)</li> </ul>	12 - 13 Hours	12 Hours	12 Hours	12 Hours
<ul style="list-style-type: none"> <li>Able to support dual monitor display, i.e. simultaneous display to internal monitor and external monitor/AV.</li> </ul>	Yes - HDMI	Yes Via HDMI and USB C	Yes Via HDMI and USB C	Yes Via HDMI and USB C
<ul style="list-style-type: none"> <li>High definition resolution at a minimum (720x1280 or better)</li> </ul>	1366 x 768 HD	1366 x 768 HD	1366 x 768 HD	1366 x 768 HD
<ul style="list-style-type: none"> <li>Capable of simultaneous moderate-intensity tasks and running the standard/curricular software provided</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>Capable of capturing visual and audio content using inbuilt facilities</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>Configured with a single image that can be used securely and safely 'out of the box' where required</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>All devices provided must have integrated, non-detachable batteries</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>11.6" screen (10" minimum for Tablet form factor)</li> </ul>	11.6"	12.5"	12.5"	12.5"

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

Crown Copyright 2018

- Dual core CPU minimum (Quad Core preferred) (Laptop) / Dual Core CPU minimum (Tablet)
- o PassMark CPU benchmark of 2,200 preferred (<https://www.cpubenchmark.net/>)
- o Must be current generation processor

Intel Celeron  
N4120 -  
PassMark  
2440 -  
Current

Intel Celeron  
N3450 with  
Intergrated  
GPU.

Intel Celeron  
N3450 with  
Intergrated  
GPU.

Intel Celeron  
N3450 with  
Intergrated  
GPU.

- 4Gb RAM

4Gb

4Gb

4Gb

4Gb

- 64Gb SSD, SSD and Firmware must be able to support DISM imaging

64Gb SSD  
HDD

64GB eMMC

64GB eMMC

64GB eMMC

- Webcam VGA (480p minimum), 720p or greater preferred

1366 x 768

1366 x 768

1366 x 768

1366 x 768

- Headphone/microphone socket

Yes

Yes

Yes

Yes

- Wifi to 802.11ac minimum

Yes

Yes

Yes

Yes

- Internal Speaker(s)

Yes

Yes

Yes

Yes



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

Crown Copyright 2018

- 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; - the Buyer requires the option to purchase tablets with an attachable/detachable keyboard - prices should be provided for the tablets with and without a keyboard.

- 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 supplied.

yes x 2 USB 3.0 Type A (No USB-C). USB-A ports can be used for charging peripherals devices.	1 Mini SD Slot, 2 x USB 3.0, 1 x Type C (power/data/display)	1 Mini SD Slot, 2 x USB 3.0, 1 x Type C (power/data/display)	1 Mini SD Slot, 2 x USB 3.0, 1 x Type C (power/data/display)
Yes	Yes	Yes	Yes
Factory Enabled – Microsoft requires that OEMs submit Computer Build Reports to register the Windows 10 Digital Product Key (DPK/PKID). Microsoft best practice for Autopilot registration is for OEMs to register devices via the OEM API on behalf of the customer. This is done by submitting the device	PKID/Hardware Hash at factory - A batch file is available to include all device specifics as well as outerbox	PKID/Hardware Hash at factory - A batch file is available to include all device specifics as well as outerbox	PKID/Hardware Hash at factory - A batch file is available to include all device specifics as well as outerbox

<p>data (the DPK) along with the Customer Tenant ID and Azure Domain ID, once the customer has consented to Dell doing this for them. Use of this approach ensures that devices are trusted for management via the Device Firmware Configuration Interface (management of BIOS settings via Intune). Devices that have been uploaded utilising the hardware hash by customers into their own tenant will not be trusted for this level of management.</p>			
---	--	--	--

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

Crown Copyright 2018

<ul style="list-style-type: none"> <li>Minimum 1-year warranty return to base – manufacturer turnaround time to be outlined in the Price Schedule document</li> </ul>	Priced with 1 year basic onsite warranty M-F 08:00-18:00 after tech support diagnosis - NBD (See Basic Hardware service doc).	1 Year Warranty	1 Year Warranty	1 Year Warranty
<ul style="list-style-type: none"> <li>Appropriately sized sleeve case for device (e.g. 11.6" sleeve for an 11.6" form factor laptop, etc)</li> </ul>	Supplied	Supplied	Supplied	Supplied
<ul style="list-style-type: none"> <li>Windows 10 Professional Education version 2004. 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</li> </ul>	Windows 10 Pro v 2004	Windows 10 Pro 2004 Education with No S Mode or bloatware	Windows 10 Pro 2004 Education with No S Mode or bloatware	Windows 10 Pro 2004 Education with No S Mode or bloatware
<ul style="list-style-type: none"> <li>Recovery partition must be present on the devices</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>No bloatware on main or recovery partitions – Desirable requirement</li> </ul>	Compliant	Compliant	Compliant	Compliant
<ul style="list-style-type: none"> <li>Video port</li> </ul>	Yes	Yes	Yes	Yes

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

Crown Copyright 2018

<ul style="list-style-type: none"> <li>PSU fitted with UK 3-pin as standard</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>Security features – confirm TPM2 minimum requirement</li> </ul>	TPM 2.0	TPM 2.0	TPM 2.0	TPM 2.0
<ul style="list-style-type: none"> <li>Software image consistency 12 month minimum</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>SCCM support driver pack must be available</li> </ul>	Yes	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>BIOS: <ul style="list-style-type: none"> <li>UEFI and evergreen commitment</li> <li>Network boot (PXE) must be possible via readily available Ethernet adapter if no ethernet port available on the devices</li> <li>DISM imaging must be possible</li> <li>Remote management / scriptable BIOS passwords desirable</li> <li>Once an admin BIOS password is set, the BIOS can only be altered with that password and through no other means or work around</li> </ul> </li> </ul>	Yes	EUEFI & Evergreen Supported. Remote management and PXE not supported.	EUEFI & Evergreen Supported. Remote management and PXE not supported.	EUEFI & Evergreen Supported. Remote management and PXE not supported.
<ul style="list-style-type: none"> <li>Compliancy – energy star certified or EPEAT</li> </ul>	Energy Star 6.1	Yes	Yes	Yes
<ul style="list-style-type: none"> <li>Where an inbuilt PXE compatible RJ45 socket is not available on a laptop device the Buyer requests optional pricing for PXE Compatible RJ45 to USB adapters that will operate with laptop device models put forward</li> </ul>	Optional adapter listed in the pricing schedule	Optional adapter listed in the pricing schedule	Optional adapter listed in the pricing schedule	Optional adapter listed in the pricing schedule

## Annex B – Chromebook Specifications

Device Requirement - Minimum Specification	Google Chromebook Model 1	Google Chromebook Model 2	Google Chromebook Model 3
Make / Model (SKU)	HP Chrome 11 2D338EA / 9VZ08EA / 9VZ09EA / 9VZ19EA / 3C219EA / 9TX88EA / 9TX89EA / 9VX76EA	HP Chrome 14 10X49EA / 9TX90EA / 7DD00EA / 7DF07EA	Dell 3100 Chromebook - s002chb310011ukie
<ul style="list-style-type: none"> <li>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)</li> </ul>	Yes	Yes	12 - 13 Hours
<ul style="list-style-type: none"> <li>The device must be robust in design and suitable for an educational environment.</li> </ul>	Ruggedised Clamshell	Ruggedised Clamshell	Clamshell - Educational grade - rubbersized corners / keys resistant to picking / extra liquid protection. IP rating is for fully ruggedized devices only. These units have been toughened for the use by pupils as above
<ul style="list-style-type: none"> <li>11" screen minimum</li> </ul>	11.6"	14"	11"
<ul style="list-style-type: none"> <li>4gb ram</li> </ul>	4GB	4GB	4Gb
<ul style="list-style-type: none"> <li>16gb SSD HDD minimum</li> </ul>	16GB/32GB eMMC	32GB eMMC	16Gb SSD HDD

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

Crown Copyright 2018

<ul style="list-style-type: none"> <li>Wifi to 802.11ac</li> </ul>	<b>802.11ac</b>	<b>802.11ac</b>	802.11ac
<ul style="list-style-type: none"> <li>Speaker</li> </ul>	<b>Stereo speakers</b>	<b>Stereo speakers</b>	Stereo speakers
<ul style="list-style-type: none"> <li>1 x USB 3.0 Type A socket and 1 x USB 3.0 Type C socket</li> </ul>	<b>2 x USB 3.1 Type-C ; 2 x USB 3.1 Gen 1</b>	<b>2 USB 3.1 Type-C™ Gen 1 (Power delivery, DisplayPort™); 2 USB 3.1 Gen 1 (HP Sleep and Charge)</b>	2 x USB-A / 2 x USB-C
<ul style="list-style-type: none"> <li>Keyboard</li> </ul>	<b>Standard UK Keyboard</b>	<b>Standard UK Keyboard</b>	Standard UK Keyboard
<ul style="list-style-type: none"> <li>HD Webcam (720p or greater)</li> </ul>	<b>HD Webcam</b>	<b>HD Webcam</b>	HD 1280 x 720
<ul style="list-style-type: none"> <li>Headphone/microphone socket</li> </ul>	<b>1 x Stereo headphone/microphone combo jack</b>	<b>1 Stereo headphone/microphone combo jack</b>	Yes
<ul style="list-style-type: none"> <li>Minimum 1-year warranty return to base – manufacturer turnaround time to be outlined in the Price Schedule document</li> </ul>	<b>1 year standard</b>	<b>1 year standard</b>	Priced with 1 year basic onsite warranty M-F 08:00-18:00 after tech support diagnosis - NBD (See Basic Hardware service doc).
<ul style="list-style-type: none"> <li>Appropriately sized Sleeve case for the device</li> </ul>	<b>11"</b>	<b>14"</b>	Supplied
<ul style="list-style-type: none"> <li>Device management license for remote cloud administration shall be included</li> </ul>	<b>Yes</b>	<b>Yes</b>	Yes

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

Crown Copyright 2018

- PSU fitted with UK 3-pin as standard

Yes

Yes

UK 3 Pin Power  
with 65W AC  
Adapter. USB-C  
power adaptor

- HD minimum screen resolution (720 x 1080 minimum)

**HD****HD**

1366 / 768 HD

- Compliancy energy star certified or EPEAT

ENERGY STAR® certified

ENERGY STAR® certified

Energy Star 7.0

- Google Chrome Education Upgrade Licences must be included in the unit price submitted

Yes

Yes

Yes

**Annex C – iPad Specifications**

Device Requirement - Minimum Specification	Apple iPad Model 1
Make / Model (SKU)	Apple iPad 8th Gen - MYL92B/A
Apple 10.2-inch iPad Wi-Fi 32GB (7th Generation Minimum, 8th Generation Preferred)	8th Gen
Appropriately sized sleeve case for device (e.g. 11" sleeve for iPad, etc)	Supplied