Crown Commercial Service

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 16/06/2021 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**").

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms.

The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website; http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm6100.
The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

13. the Framework, except Framework Schedule 18 (Tender);
14. the Order Form;
15. the Call Off Terms; and
16. Framework Schedule 18 (Tender).

Crown Commercial Service

Section A
General information

Contract Details	
Contract Reference:	CCIS21A25.
Contract Title:	Services Partner for the Get Help With Technology Service
Contract Description:	Customer Management, Logistics and distribution of devices.
Contract Anticipated Potential Value:	Up to a maximum of £9,000,000.00 (ex VAT) including all extension options
Estimated Year 1 Charges:	Up to a maximum of £9,000,000.00 (ex VAT) including all extension options
Commencement Date:	Monday 11th October 2021

Buyer details

Buyer organisation name
Department for Education.

Billing address
Department for Education
Sanctuary Buildings
20 Great Smith Street
London
SW1P 3BT

Buyer representative name:
REDACTED (Personal Information)

Buyer representative contact details:
REDACTED (Personal Information)

Crown Commercial Service

Supplier details
Supplier name Computacenter (UK) Limited **Supplier address** Computacenter UK, Hatfield Avenue, Hatfield Business Park, Hatfield, AL10 9TW **Supplier representative name** REDACTED (Personal Information) **Supplier representative contact details** REDACTED (Personal Information) **Order reference number or the Supplier's Catalogue Service Offer Reference Number** CCIS21A25

Guarantor details
Guarantor Company Name Not Applicable **Guarantor Company Number** Not Applicable **Guarantor Registered Address** Not Applicable

Crown Commercial Service

Section B

Part A – Framework Lot

Framework Lot under which this Order is being placed	
1. TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2. TRANSITION & TRANSFORMATION	☐
3. OPERATIONAL SERVICES	
a: End User Services	x
b: Operational Management	☐
c: Technical Management	☐
d: Application and Data Management	☐
5. SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
Monday 11th October 2021

Contract Period
Monday 11th October 2021– Friday 1st April 2022 for the initial contract term.

Initial Term Months	**Extension Period (Optional)** Months
Six (6) Months	Two periods of three (3) months (6+3+3)

Minimum Notice Period for exercise of Termination Without Cause
30 Days (Calendar days)

Sites for the provision of the Services
The Supplier shall provide the Services from the following Sites: Supplier Premises listed below.

Buyer Premises:
Not Applicable

Supplier Premises:
Primary Integration Centre in Hatfield – Hatfield Avenue, Hatfield Business Park, Hatfield, AL10 9TW
Secondary Integration Centre in Braintree – Address TBC by Supplier

Third Party Premises:
Not Applicable

Crown Commercial Service

Buyer Assets

DATA: The Buyer will supply the supplier with the necessary details of Settings/Responsible Bodies named contact, and address details for delivery of devices. The Supplier will grant authority to the Supplier to collect additional data assets from Settings and responsible Bodies as required for the successful delivery of the service.

No other areas will apply

Additional Standards

Standards to be applied as those stated with ICT policy attachment below;

I. All Supplier contacts are required to be cleared to a minimum of BPSS (Baseline Personnel Security Standard) standard with demonstrable ISO27000 security controls established.
II. Data residency to be UK / EU territory only.

Commercially Sensitive Standards;

III. In this section, 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.
IV. 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).
V. 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
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
4	Commencement Date	Attachment 3 Specification of Requirements	Duration of the Contract

Buyer Security Policy

Please refer to Annex A – DfE Security Clause for full details. Security policy compliance is based on the provisions that are only relevant to the agreed solution that will be finalised during the co-design phase of Implementation

Buyer ICT Policy

Please refer to Annex B – Buyer ICT Policy for full details.

Insurance
As per the standard terms in the framework

Buyer Responsibilities
The Buyer will provide data and information as required by the supplier to monitor allocations and deliver devices to the correct location.

Goods
Not applicable

Governance – Option Part A or Part B

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	x
Part B – Long Form Governance Schedule	☐

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	x
Part B – Long Form Change Control Schedule	☐

The Part selected above shall apply this Contract.

Crown Commercial Service

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses

Part A – Additional Schedules

Additional Schedules	Tick as applicable
S1: Implementation Plan	x
S2: Testing Procedures	x
S3: Security Requirements (either Part A or Part B)	Part A
S4: Staff Transfer	☐
S5: Benchmarking	☐
S6: Business Continuity and Disaster Recovery	x
S7: Continuous Improvement	x
S8: Guarantee	☐
S9: MOD Terms	☐

Part B – Additional Clauses
Not Applicable to this contract.

Additional Clauses	Tick as applicable
C1: Relevant Convictions	☐
C2: Security Measures	☐
C3: Collaboration Agreement	☐

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses
Not Applicable to this contract.

Alternative Clauses	Tick as applicable
Scots Law	☐
Northern Ireland Law	☐
Joint Controller Clauses	☐

Crown Commercial Service

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)
Security Plan to be completed within three (3) weeks of Contract commencement or by 28 October 2021, whichever is soonest.

Additional Schedule S4 (Staff Transfer)
Not Applicable

Additional Clause C1 (Relevant Convictions)
Not Applicable

Additional Clause C3 (Collaboration Agreement)
Not Applicable

Crown Commercial Service

Section D
Supplier Response

Commercially Sensitive information
Contents of the Supplier's Bid Submission.

Supplier's Technical Response

REDACTED (Personal Information)

Section E
Contract Award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

Name	REDACTED (Personal Information)
Job role/title	REDACTED (Personal Information)
Signature	REDACTED (Personal Information)
Date	**8th October 2021**

For and on behalf of the Buyer

Name	REDACTED (Personal Information)
Job role/title	REDACTED (Personal Information)
Signature	REDACTED (Personal Information)
Date	**11th October 2021**

Crown Commercial Service

Attachment 1 – Services Specification

PURPOSE

- The Contracting Authority requires a Services Partner for the customer management, logistics and distribution of devices to schools on behalf of the Get Help With Technology Service. The services to be provided will include;
    - Receipt and stock management of the devices procured for the scheme from Devices Suppliers.
    - Working with the Contracting Authority to support the testing of each make/model of device to ensure that they adhere to the Contracting Authority's Devices Minimum Specifications.
    - Managing the shipment of stock to schools
    - operating the "Swap" service, where schools have accidentally ordered the wrong devices, and Dead on Arrival (DoA) service for devices that are damaged or not functioning as expected at the point of delivery,
    - the provision of customer facing services to schools and Children's Social Care providers,
    - providing up to date, ideally real-time, reporting back to the Department in relation to the stock and flow of devices to Settings.

BACKGROUND AND OVERVIEW OF REQUIREMENT

- Since the first national lockdown and closure of schools resulting from the Coronavirus pandemic, in March 2020, the Department for Education (DfE) has provided over 1.3 million laptops and tablets to disadvantaged children in years 3 to 13 who would not otherwise have access to remote education or who are being supported by a social worker. These have been delivered via the Get Help With Technology Programme.
- A proportion of Windows devices were delivered with a temporary secure custom build, though with the intention that the 'DfE build' will be replaced with a build best suited to the organisational and end user needs. For this 'wave 8' round of device procurement there is no need for a custom build so all devices will be as supplied by manufacturers.
- DfE is not anticipating further school closures on a national scale. However, ongoing, localised, disruption to face to face education resulting from the pandemic is likely (especially during the Autumn/Winter 'flu season') and so ensuring that schools can offer support to disadvantaged and vulnerable children with remote education remains a priority for DfE.
- DfE has now secured funding to purchase a further wave of circa 500,000 devices to support disadvantaged children without access to devices in the event of further disruption to face to face education resulting from the pandemic.
- Should further disruption resulting from the pandemic be minimal, these devices will need to be useable by schools and children more generally in support of in-school and home learning.
- The tender includes an assessment of Social Value to be delivered by the Services Partner during the term of the contract. For this contract Social Value will be assessed as 'Improving

Health and Wellbeing' for staff working on this contract and 'Tackling Economic Inequality'; with reference to creating employment opportunities, particularly for those who face barriers to employment and/or who are in deprived areas.

- Support for educational attainment relevant to the contract, including training schemes that address skills gaps and result in recognised qualifications will also form part of this assessment.
- The Department for Education, henceforth referred to as the Contracting Authority, are currently procuring 500,000 devices (laptops and tablets) from OEMs and device resellers (via a separate procurement process).
- It will be the responsibility of Device Suppliers to arrange for importation of these devices and for bonded storage in the UK until they become the responsibility of the Services Partner, for onward distribution to Responsible Bodies and Settings.

Crown Commercial Service

DEFINITIONS

Expression or Acronym	Definition
Allocation	The maximum number of devices an RB or Setting can order; the allocation number for each RB/Setting is set by DfE.
Authorised Contact	The initial user from an RB or Setting, which will be provided by DfE. The initial user may add further Authorised contacts to act on behalf of their RB or Settings, including individuals from third parties.
Business Day	Between 7am and 10pm each week day (Monday to Friday excluding Bank Holidays).
Caps	A portion of the Allocation up to which Settings can order within a given timeframe (e.g., they may be able to order 1/3 of their total allocation within a given month so this would be the 'cap' at that time).
Contracting Authority	The Government Department for whom the service is being procured, in this case the Department for Education (DfE)
Dead on Arrival (DoA)	Dead on Arrival means a Device that is received damaged or not fully functional, and discovered within 10 days of receipt at the RB/Setting (DoA does not apply to Routers). A device arriving damaged to a Services Partner location, including devices where the security seal has been compromised.
Device	Any device procured by DfE for use in education or Social Care. This includes Windows Laptops, Windows Tablets, Chromebooks, iPads and Android Tablets.
Device Minimum Specifications	Minimum specifications that devices of each type must meet to be procured and distributed by the Programme, as issued by the Contracting Authority.
Device Suppliers	Device Resellers or OEMs contracted (via a separate procurement process) to supply devices to the scheme.
OEMs	Original Equipment Manufacturers
Responsible Body (RB)	Organisation responsible for the management of schools, colleges or social care workers
Router	4G wireless router (no SIM, not configured) purchased under a previous Wave and still available for Settings to order.

Service Hours	Ordering Platform: Monday to Friday, 7am until 10pm (excluding bank holidays) Customer Support: Monday to Friday, 8am until 6pm (excluding bank holidays)
Settings	Individual organisations with responsibility for children and young people: school, college or social care
Tablet	Windows tablet, iPad, Android tablet
Tablet bundle	Means a Tablet and its protective sleeve (in order to fulfil orders quickly, sleeves may be dispatched separately)

SCOPE OF REQUIREMENT

- The Service Partner will need to be able to provide the following associated services:
  - Building, managing, validating and maintaining the shared database required to support the service.
  - Provide an ordering platform to enable RBs and Settings to order the right types of devices in appropriate numbers (some additional users are ICT suppliers to whom RB/Settings have delegated responsibility for ordering devices).
  - Work with Device Suppliers to manage inbound stock, the Services Partner will take responsibility for the devices from Devices Suppliers early in the contract and thenceforth following importation to the UK by Devices Suppliers.
  - Preparing devices ahead of dispatch to Settings, to include quality assurance and production of additional accompanying materials. Devices will ship individually in their boxes.
  - Arranging for transport of devices to Settings; to include tracking and monitoring of stock in transit and confirmation that devices have been safely received.
  - Operate the "Swap" service – where schools have accidentally ordered the wrong devices – and the Dead on Arrival (DoA) service for devices that are damaged or not fully functional at the point of delivery. Device Suppliers will have to replace these under the terms of their contracts with the Department.
  - Providing a customer facing service to all customer groups using the service for ordering devices and for support with resolving any problems arising with device shipments and deliveries.
  - Providing up to date reporting of the stock, flow and status of devices back to the Contracting Authority, ideally in real time, to enable governance and oversight of the programme.

- The Contracting Authority is seeking Optional Pricing for the preparation, printing, and packaging of additional printed materials to assist schools with use of the devices (see para □o□ for full details below).
- As stated at section □o above, the procurement of new devices for the scheme is being undertaken separately. Device Suppliers winning contracts under that (separate) procurement will be responsible for holding the devices in bonded storage until the Services Partner becomes responsible for them.
- The Supplier will need to comply with DfE information management and security protocols throughout delivery of the requirement (see Section 0).
- Any external communications produced to promote any services being delivered on behalf of the DfE, such as marketing materials, advertisements and press releases Shall follow the branding and communications guidelines provided by the DfE and Shall be approved by the Press Office.

THE REQUIREMENT

- The Contracting Authority expect to have contracts signed with Device Suppliers by mid-September, with the intention that responsibility for the devices will transfer over to the Services Partner from mid-October for distribution to schools.
- The Supplier will need to be in a position to deliver devices to RBs/Settings shortly after they are received from device suppliers. DfE will determine which RB/Settings can order devices and the number of devices they can order. The schedule for inviting settings to order will be determined by DfE in the Autumn and will be subject to change for the lifetime of the contract. The supplier must, therefore, be able to store devices, potentially for an extended period, prior to settings being invited to order. This may involve storing the full quantity of 500,000 devices for a period.
- Manufacture to order devices will take longer to be available and are likely to be delivered in tranches between November and the critical date for Device Suppliers to have all of their contracted stock available for distribution, 17 December 2021. At the peak of activity, up to 100,000 devices may be required to be distributed to Settings in a single week.
- It is anticipated that the service for managing the distribution of devices to schools will need to be fully ready from mid-October.
- The sections outlined below detail the services required. These services will need to be delivered holistically, as a single user journey, from ordering to receipt of devices, rather than users experiencing 'hand-offs' to sub-contractors. The Contracting Authority will require the Services Partner to engage with User Research activity to develop the service and user journey.
- **Building, validating and managing the underlying database for providing the service.**
  - The Supplier will work with DfE to maintain a central, shared view of all RBs and Settings and data to support delivery of the service (Annex A).
  - The database must be capable of supporting the relationships between RBs and Settings (Annex B), including the ability for example, of RBs to order on behalf of Settings whilst maintaining accurate and robust data for every RB and Setting. [Annex B provide relationship map (already exists)

- Authorised Contacts must be able to update key details held in the database (see Annex A)
- The Supplier will need to support a minimum of 3 Authorised Contacts per Setting and a minimum of 5 Authorised Contacts per RB

- **Provide an ordering platform**
  - The Supplier will need to provide a secure online ordering platform to enable Authorised Contacts to order the following from the service:
    - Devices (laptops and tablets)
    - 4G routers
  - The ordering platform must be configurable to include (but not be limited to):
    - brief descriptions of items available
    - the relationships between RBs and Settings (Annex B),
    - limits on ordering quantities (Allocations and Caps), and
    - adjustment of relationships and ordering quantities during the service, for individual and related RBs and Settings
    - ordering a mixture of device types and routers
    - Splitting an order across multiple shipping destinations
    - prioritisation of specific orders at DfE's request
    - changes to items available (e.g., removal, replacement, additions)
    - 'promotional' (banner) text to highlight key messages / updates about the service.
    - allow RBs and Settings to order and register Chromebook licences (against one or more domains)
    - other items as agreed during mobilisation and service
  - The Supplier must be able to integrate and synchronise data via a secure approach (e.g., API or downloads from the GHwT service) to operate at significant pace and scale whilst maintaining data integrity between the supplier and Contracting Authority. See Annex A for data exchanges.
  - Prototypes and staging areas need to be made available by Suppliers to test the systems supporting the service from end-to-end.
  - The Supplier will need to provide RBs/Settings with their current ordering data and a view of the historic ordering activity (order placed and user) and notify the RBs/Settings of changes to their ordering status, for example to confirm order is placed, changed, dispatched and delivered, including the relevant information.

- The Supplier will need to support, identify and update contacts where required.
- As a minimum, the online ordering platform should be open and available for ordering every Business Day during Service Hours.
- Planned maintenance and development of the platform should take place outside Service Hours for platform availability usually with three days advance notice to DfE and service users.
- The platform will need to adhere to the Contracting Authority's information security requirements (see Section 0)

- **Enabling Device Ordering**
  - The Supplier will need to provide clear, up-to-date guidance for RBs/Settings about how to use the service ahead of ordering. This should include (but not be limited to):
    - Account management
    - How to place an order
    - How to amend an order
    - Order status
    - Important information & Checklists (e.g., How to check items received, report faults & issues including device Dead on Arrival (DoA) devices)
    - How to report a delivery issue
    - Device specific information
    - Chromebook licence ordering and registration
    - Router set up guide
  - Due to expected high volumes, the end-to-end ordering process should be automated wherever possible to maximise efficiencies. The Supplier should proactively seek out and recommend opportunities for further efficiencies during the contract term (see Section 10).
  - Authorised Contacts should be able to use the portal to choose a suitable date during school term time to receive devices at a delivery address associated with their Setting.
  - The Contracting Authority will need the Supplier to be ready to accept 'manual orders' for devices to RBs/Settings. These orders would be manually issued centrally from the Contracting Authority, and not placed through an ordering platform. The expectation is fewer than 1% of orders will be manual.
  - The Contracting Authority will need the Supplier to be ready to accept 'priority orders' for devices from RBs/Settings. RB/Settings will be prioritised by the Contracting Authority and invited to order when criteria are met, for example if an RB/Setting becomes heavily reliant on remote education during a local lockdown.
  - Authorised Contacts must be able to log into their account, even if their RB/Setting is not able to order (e.g., because they have reached their cap), so there must be clear information about what they are able to do (e.g., update their details) and what they cannot do (e.g., place further orders).

- The user experience of the Supplier system must be tailored specifically for the programme and for use by the Authorised Contact.
- All aspects of the platform must be accessible to users with a range of additional access needs, and comply with best practice, in line with WCAG 2.1 AA guidelines.

- **Storage and stock management**
  - At an agreed interval following contract commencement, the Services Partner will become responsible for stock procured from Devices Suppliers and held in the UK. The Services Partner may request that stock be physically moved to a preferred warehouse location or may reach an alternative agreement with Devices Suppliers.
  - The Supplier will be expected to be able to store up to a maximum of 500,000 units at any one time, either in their own warehouses or via arrangements with a third-party. However, this quantity of storage is only likely to be required for a short period, until stock starts being shipped to schools, potentially in large volumes. We are, therefore, keen to have options to pay for storage monthly, according to the number of units remaining in storage.
  - The Supplier will be required to arrange suitable insurance for devices from the point at which they accept responsibility for them until the time when they have been successfully delivered to Settings.
  - The Supplier should be able to work with Device Suppliers to track and monitor numbers and types of stock available and inbound and to identify future pressures on stock in relation to specific devices.
  - Stock positions, and the flow of stock, will need to be easily viewable by the Contracting Authority, ideally in real-time. Key reports include, but are not limited to:
    - stock held,
    - stock committed against orders (pending dispatch)
    - stock dispatched, and;
    - stock received by RBs and Settings
    - stock returned (returned from RBs and Settings)
    - stock expected to return (notified by RBs and Settings but not received
    - on request, the shipped location of individual stock items (e.g., by unique serial number).
    - on request, details against any order placed (e.g., serial numbers of devices for an individual school and their current location).
  - The Service Partner will be required to supply regular reports. The data provided may be used in official government publications and therefore must be accurate, reliable, and auditable. A list of reports required is provided in Section 8.

- **Storage and distribution of Routers already owned by the Programme:** Although the programme will not be offering a centrally procured connectivity solution from the Autumn, we currently own circa 24,000 4G routers which we would like the Services Partner to warehouse and distribute to schools requesting these. We are, therefore, seeking an option on storage and distribution costs of these routers to be itemised separately within Bids.

- **Preparing devices pre-dispatch**

  - The Services Partner will need to select (randomly) up to six devices from each new device type or Stock Keeping Unit (SKU) from the first delivery of any new make/model to support assurance that new SKUs meet the Contracting Authority's Device Minimum Specifications, and to identify any operational device related issues that may arise as early as possible. The Services Partner will be expected to collaborate closely with technical specialists working for, or on behalf of, the Contracting Authority in relation to this testing. We are interested to hear any further offers for how Bidders can support testing of new SKUs against the Device Minimum Specifications for each device type. These are listed in Annex F.
  - The Devices Supplier is expected to deliver Devices in security-sealed boxes; one Device per box. The Services Supplier must ensure the boxes remain intact and security sealed for outbound deliveries.
  - Where devices are supplied with sleeves, the Devices Supplier should, ideally, include sleeves within the same box as the device. However, there may be instances where this is not possible. The Services Partner may, therefore, need to supply sleeves for devices in separate packaging alongside Devices or, where there is a constraint on the supply of sleeves, in a separate delivery after devices have been supplied to Settings. However, sleeves should never be supplied to Settings ahead of Devices.
  - The Supplier must be capable of purchasing and supporting the registration of Chromebook education licences. Where an RB/Setting orders a device with a licence, the licence must be purchased and ready for registration at or immediately before the devices are delivered to the RB/Setting.
  - The Supplier will need to be able to appropriately label boxes to ensure that the contents of the box and order number are shown along with the Setting's address.
  - **OPTIONAL REQUIREMENT**: DOCUMENTATION DELIVERY
    The Contracting Authority is seeking Optional Pricing for the preparation, printing, and packaging of additional black and white printed materials to assist schools with use of the devices. We anticipate that these materials will be placed in self-adhesive, sealable envelopes securely attached to the outside of individual device boxes, rather than requiring the sealed boxes to be unwrapped. Printed materials within each envelope are not expected to exceed four sides of A4. It is anticipated that this requirement could apply to circa 50,000 devices. We are keen that Bidders explain how their print and packaging solutions can be delivered in an environmentally sustainable manner.

- **Dispatch and transport to Settings**

- The Supplier will need to handle orders according to priority (see para 6.6.7 and 6.7.6), with high priority orders being processed first, with other orders processed on a first-come first-served basis.
- The Supplier will be responsible for transporting items securely to Settings but may sub-contract this to a trusted third party. However, any delivery service should advise the recipient that the items are in transit and provide a delivery window for when they are expected to arrive at destination.
- The Supplier will be responsible for arranging suitable insurance for items in transit.
- The Supplier must be able to work as an extension of the OEM's supplying devices (perhaps via a Reseller) to enable adjustment of the Warranty so that it is only activated at the point of receipt by the RB/Setting.
- The Supplier must ensure RBs/Settings are enabled to request Warranty services from the OEMs (RBs/Settings are seen as the purchasers of the Devices for Warranty purposes)
- The actual number of Devices and orders per week may vary significantly and therefore a flexible model will be required. It is envisaged that 100,000 devices would represent the maximum ever likely to be required to ship in a single week.
- The Contracting Authority expects fulfilment of orders within 5 working days unless a setting requests delivery at a later date. Ideally most orders should be completed (delivered to an RB/Setting) next day on orders placed by 12pm.
- Where the Contracting Authority has requested that an order be prioritised, we expect delivery to a setting within a maximum of 2 working days.
- The Supplier should consider academic holidays and working hours when planning deliveries and collections to minimise failed attempts. The Supplier and the Contracting Authority will agree any pauses in the service in advance, so that schools can be given notice of this in good time.
- The Supplier must obtain and record proof of delivery. These records must be made available to RBs/Settings and the Contracting Authority on request.

- **Provide return logistics in cases where Settings have either ordered the wrong devices or received Dead on Arrival (DoA) devices.**
  - In cases where the wrong device type has been ordered by an RB/Setting, the Supplier may be requested to swap unboxed devices from one type to another at a particular delivery location. The Supplier must enable RBs/Settings to make the swap request and will be responsible for completing the request. In the case of Chromebooks, licences may need to be reset before they are restocked and made available to other schools. We are interested to hear from Bidders how they would appropriately manage the reintroduction of these devices to the stock to make them available to other schools.
  - For any devices that are obviously damaged upon arrival at the Service Partner's premises, the Device Supplier should be notified, and the device returned to the Device Supplier for replacement in accordance with appropriate SLAs.
  - The Services Partner will be the first point of contact for RBs and Settings to report DoA devices for replacement. The Services Partner will be responsible for return logistics from RBs and Settings for devices that are DoA. DoA devices

need to be returned to Devices Suppliers for replacement, in line with the Devices Supplier contracts and SLAs.

- Devices swapped in this process must be suitably quarantined and the Services Supplier must work directly with the Device Supplier for the return and replacement of DoA devices.
- We are interested to hear from Bidders how they would operate the DoA process, as set out in Annex D, with minimal involvement, disruption and cost to Settings. The RB/Setting must not be charged for returning devices under DoA, even if the device is found to be in full working order and undamaged by the Device Supplier.

- **Providing a customer-facing service for Settings**

  - The Supplier will be responsible for resolving queries pertaining to any part of the service for which the Supplier is responsible, an initial response should be provided within 3 business days and satisfactory resolution of the issue should be achieved within 6 business days.
  - The Supplier will receive requests pertaining to their part of the service via the Contracting Authority's existing user support system (Zendesk). Annex C gives the breakdown of enquiries for the service between August 2020 and June 2021.
  - The Supplier will supply the Contracting Authority with any new response templates (macros) that they generate that may help the Contracting Authority to speed up resolution of common requests, for approval.
  - Devices Suppliers have been asked to provide an option for extended Warranties (2/3 years) at a discounted price to RBs and Settings. The Supplier will work with OEMs and Resellers to secure a clear means by which RBs/Settings can purchase the enhanced warranty, though this may be via a third-party agreement.
  - All customer-facing communication must match DfE style and tone and have approval from the Contracting Authority before issuing.

- **Reporting**

  - The Supplier shall be responsible for reporting key Management Information back to the Contracting Authority in line with the requirements for monitoring Contract KPIs and SLAs.

KEY MILESTONES AND DELIVERABLES

- The following Contract milestones/deliverables shall apply:

Milestone/ Deliverable	Description	Timeframe or Delivery Date
2	Draft Delivery plan, including key assumptions	On date of contract signature
3	Draft Customer support resource plan & processes	On date of contract signature
4	Draft Business process map, including data flows	Within week 1 of Contract signature

5	Draft Governance & reporting plan	Within 1 week of Contract signature
6	Key contacts	Within 1 week of Contract signature
7	Third party agreements (redacted)	Within 2 weeks of Contract signature
8	WCAG 2.1 AA Compliance assessment, report and actions	Within 4 weeks of Contract signature
9	Co-design workshops	Within 1 day of Contract signature
10	Order platform – available & configured	Within 3 weeks of Contract signature
11	Database and system environment to be made available for third party testing.	Within 3 weeks of Contract signature
12	All systems and interfaces, built, tested & ready for use (Service go-live)	No later than 1 Nov 2021
13	Draft exit plan	Within 3 weeks of Contract signature
14	Final Exit plan	Within 2 months of Contract signature

MANAGEMENT INFORMATION/REPORTING

- The Supplier should provide daily update reports on individual orders received and orders dispatched in a format and via a secure service to be agreed with the Contracting Authority. Such reports must include all data required to aggregate orders and dispatches by individual RBs and Settings and include the following information;
  - device category (e.g. 'persona');
  - device manufacturer and model;
  - unique order IDs and
  - unique organisation IDs (drawn from DfE's 'Get Information About Schools (GIAS)' service).
- The Contracting Authority must also be able to access data and reports on the service levels and user support, ideally in real time but, as a minimum, updated daily for example:
  - Orders placed, in transit and delivered (in total, by RB, Setting and Authorised Contact).
  - Supplier stock levels by device type daily
  - Any additional details pertaining to stock management (see □o□ to □o□)
  - Service usage by authorised users;
    - Percentage of eligible user base who have signed-in to the service
    - ordering journey start to completion ratio
    - percentage of eligible user based who have placed an order

- elapsed time - order completion to dispatch
- failed deliveries
- DoA returns processed
- Average time to replace a DoA device, from DoA request raised to replacement device arriving at a setting
- cost per transaction

▪ User support metrics should include;

- Service tickets received/resolved
- Information about how these have been triaged
- avg first response time back to a customer,
- avg time to resolution
- a user satisfaction measure

▪ User support enquiries – summary reports

▪ Supplier system performance reports

- Allocation queries escalated and resolved (Resolution rate for Allocation Queries will not be included as a KPI).

VOLUMES

- The key volumes associated with this requirement are as follows;
  - ▪ A maximum of 500,000 units to be stored at any one time out of
  - ▪ Circa 500,000 devices in total, to be processed and dispatched to;
  - ▪ Circa 22,000 schools overseen by 3,600 RBs, as well as around 150 Local Authority Children's Care Services requiring;
  - ▪ Up to 95,000 Authorised Contact accounts to be set up by a Service Partner to ensure access.
- We estimate that up to 30,000 service enquiries will be handled during the period of the contract term, with the majority being during a period of peak disruption (likely over the late Autumn/early Spring terms).

CONTINUOUS IMPROVEMENT

- The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
- The Supplier should present new ways of working to the Contracting Authority during Contract Review Meetings.
- Changes to the way in which the Services are to be delivered must be brought to the Contracting Authority's attention and agreed prior to any changes being implemented.

- The Supplier will be required to cooperate with both the Contracting Authority and wider Government initiatives aimed at improving public services. This could include (but is not limited to) Government Digital Service (GDS) Service Assessments and independent research into user-experience for users of the service.

SUSTAINABILITY AND SOCIAL VALUE

- In addition to price and the quality of a service offer, the Contracting Authority will also be assessing the Social Value under the categories of 'Improving Health and Wellbeing' for staff working on this contract and 'Tackling Economic Inequality'.

STAFF AND CUSTOMER SERVICE

- The Supplier shall provide a sufficient level of resource throughout the duration of the Contract to consistently deliver a quality service.
- The Supplier's staff assigned to the Contract shall receive suitable training and have relevant experience to deliver the Contract to the required standard.
- The Supplier shall ensure that staff understand the Contracting Authority's vision and objectives and will provide excellent customer service to the Contracting Authority throughout the duration of the Contract.

SERVICE LEVELS AND PERFORMANCE –

- For details of the proposed SLAs and performance measures, please refer to Attachment 4 in the Order Form

SECURITY AND CONFIDENTIALITY REQUIREMENTS

- All Supplier contacts are required to be cleared to a minimum of BPSS (Baseline Personnel Security Standard) standard with demonstrable ISO27000 security controls established. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
- The Supplier will be required to operate a good corporate level of security, as their back-office systems will hold and process some departmental data relating to the contract and the service provided.
- The online ordering platform used by schools will need to be sufficiently secure to resist internet and other attacks and, as such, the Supplier will need to adhere to the processes and requirements set out in Annex G below.
- Any personal information, such as contact details for departmental and school personnel, must be processed in accordance with data protection legislation.
- Data residency to be UK / EU territory only.

PAYMENT AND INVOICING

- For full details of payment and invoicing, please refer to Attachment 2 in the Order Form

Crown Commercial Service

CONTRACT MANAGEMENT

- Attendance at Contract Review meetings shall be at the Supplier's own expense. We expect these to take place fortnightly. These will usually be held remotely but the Contracting Authority reserves the right to request face to face at their discretion.

LOCATION

Devices held under management by the Services Partner, either at the Suppliers location or via a third-party sub-contractor, must be held within the UK for nationwide distribution to Settings across England.

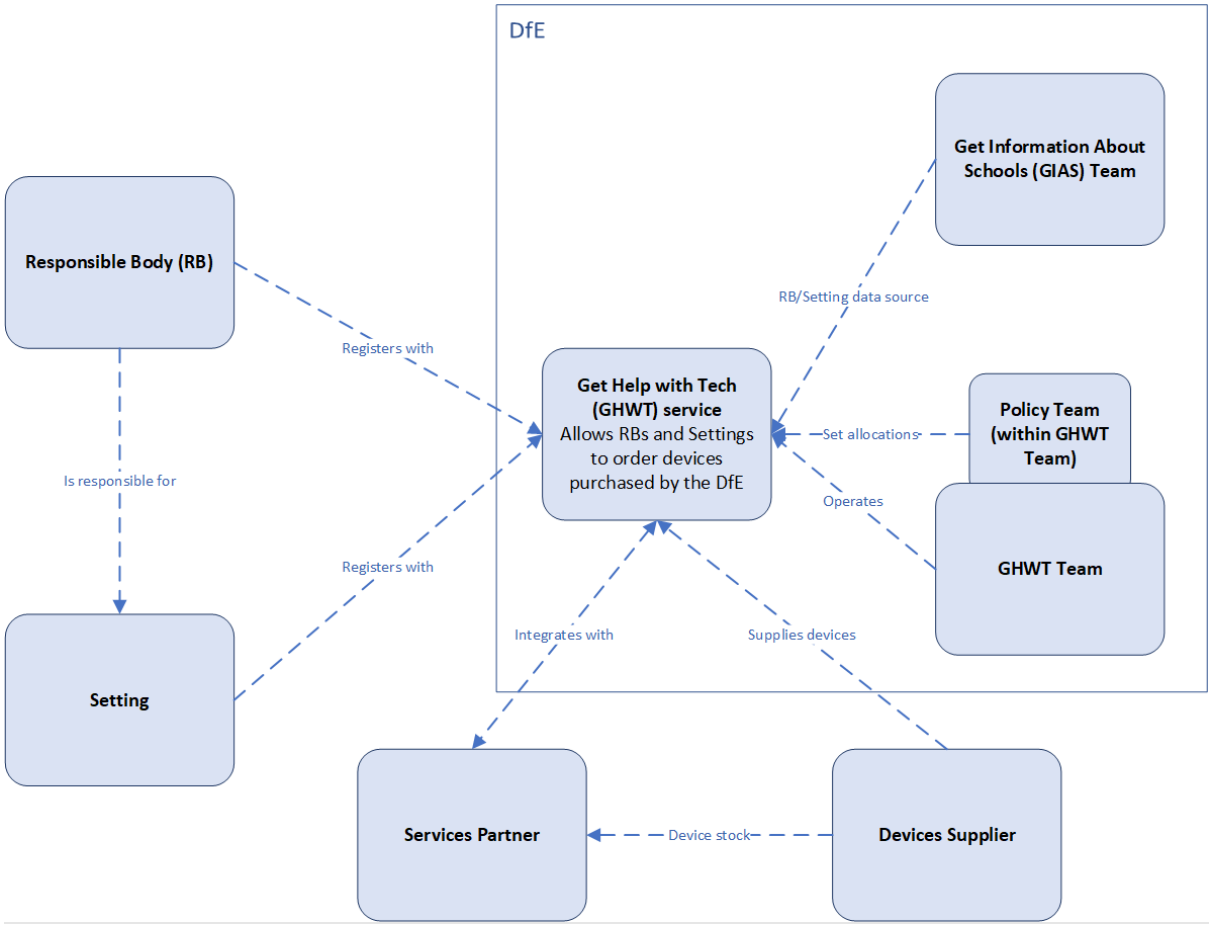
Crown Commercial Service

ANNEX A: DATA

The table below indicates the data exchanged between the Contracting Authority and the Services Partner to deliver services.

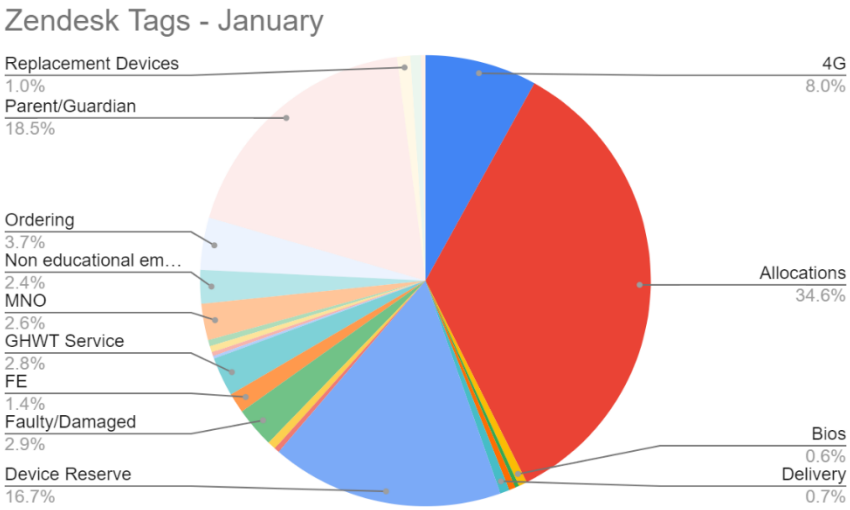
Data type	Data fields	Purpose
Authorised contacts, RBs and Settings	• First name • Last name • Email • Telephone • Responsible body name • Responsible body URN • SOLD TO number • School Name • School URN • SHIP TO number • Date of update • Time of update • Timestamp of update • Type of update	For account set up, account management and fulfilment of orders. The data will require regular updates to ensure accuracy. Scale (approx. figures) 150 Local Authorities 3,600 Trusts 17,000 Schools 430 Further Education Colleges In addition, there are a small number of other Settings, such as Independent Special Schools that may be invited to the service.
Chromebook details	• Responsible body URN • Responsible body name • School Name • School URN • Google Domain • Valid recovery off domain email address • Date • Time • RB name • RB URN • Sold to	To register licences for RBs/Settings
Allocations	• School ID • Allocation ID • Cap Type • Ship To • Cap Amount • Cap Used	To manage the number of devices RBs/Settings can, and have, ordered.

ANNEX B: RELATIONSHIPS



Crown Commercial Service

ANNEX C: CUSTOMER FACING SUPPORT (JANUARY 2021)



The above chart shows the breakdown of queries made in January 2021 when devices were made available to respond to national lockdown. Some query types will not apply for the Autumn, in particular queries from Parent/Guardian are not expected.

ANNEX D: DEAD ON ARRIVAL SERVICE

Devices arriving damaged to a Services Partner location, including devices where the security seal has been compromised, and devices which are damaged or not working as expected upon arrival with settings will be subject to the DoA process.

Upon receipt of devices, settings will be given up to 10 working days to identify whether a device was faulty at the point of arrival. After a setting has notified the Service Partner of a DoA device, or devices, the Services Partner will arrange for collection of these within 5 days of notification.

The Services Partner will then be expected to return the device to a Supplier for replacement within 3 working days of collecting it from a setting.

Device Suppliers will be expected to supply replacements back to the Services Partner within 2 working days of receiving DoA devices from the Services Partner.

Devices Suppliers will be expected to accept single and multiple (batch) DoA returns from the Services Partner.

The RB/Setting must not be charged for returning devices under DoA, even if the device is found to be in full working order and undamaged by the Device Supplier.

Devices Suppliers will be expected to accept single and multiple (batch) DoA returns from the Services Partner.

Devices swapped in this process must be suitably quarantined and the Services Supplier must work directly with the Device Supplier for the return and replacement of DoA devices

ANNEX E: PRIORITY ORDER FOR INCIDENT RESOLUTION

Priority 1 (P1) – A complete business down situation or single critical system down with high financial impact. The Buyer is unable to operate.

Priority 2 (P2) – A major component of the Buyers ability to operate is affected. Some aspects of the business can continue but it's a major problem.

Priority 3 (P3) – The Buyers' core business is unaffected but the issue is affecting efficient operation by one or more people.

Priority 4 (P4) – The issue is an inconvenience or annoying but there are clear workarounds or alternates.

Priority 5 (P5) – The issue is a background or planned task and will be addressed when time permits or on the planned date.

Crown Commercial Service

ANNEX F: DEVICE MINIMUM SPECIFICATIONS AGAINST WHICH NEW SKUS WILL NEED TO BE TESTED

Windows Laptops Device Minimum Specifications

Category	Device Requirement - Minimum Specification
Screen Size	11.6” screen minimum
Screen Resolution	Please confirm - High definition resolution at a minimum (720x1280 or better)
Multimedia	Webcam VGA 640 x 480p minimum
Connectivity	Wifi to 802.11ac minimum
Audio	Internal Stereo Speakers
Ports	2 x USB 3.0 Type A or Type C sockets - At least one USB socket to support charging/powering of peripherals/devices – the DfE will also accept 1 x USB 2.0 and 1 x USB 3.0 for the port specification - Does the device meet this specification?
Keyboard	Standard UK Keyboard
Video Port	Able to support dual monitor display, i.e. simultaneous display to internal monitor and external monitor/AV, please confirm.
Audio Ports	Headphone/microphone socket – a single 3.5mm combined Headphone/Microphone jack required
Video/audio capture	Capable of capturing visual and audio content using inbuilt facilities
Standard Warranty	Minimum 1-year warranty return to base as part of the tendered unit price.
Operating System	Minimum Windows 10 Professional Education version 2004 or 20H2 for devices available before October. S-mode not enabled.
Windows 11 Compatability	Device meets Windows 11 compatability requirements - as detailed at https://www.microsoft.com/en-gb/windows/windows-11-specifications including compatible 64bit processor
Licences	Please confirm that the operating system license is included and pre-activated for standalone use and subsequent connection of the device to a school network/domain.

UK Language pack installed with Operating System	Yes / No
Recovery Partition Present	Yes / No
Bloatware	For devices being manufactured to order, please confirm that no bloatware will be present on the main or recovery partitions or if the device has already been manufactured please provide details in the table below.
Bluetooth	Bluetooth connection
Device Encryption	Bitlocker encryption as standard
Security Features	Please confirm (TPM 2.0 Minimum Requirement)
Battery	Integrated and non-detachable - Minimum 7 hours battery life
PSU	Fitted with uk 3-pin as standard
S/W Image Consistency	12 Month Minimum
SCCM Support	Driver pack must be available - Please confirm
Autopilot	Is the Hardware Hash supplied in Intune compatible CSV format or is there an alternative mechanism that can be used by schools to generate this Hash on receipt of devices suppled to schools?
BIOS Update	UEFI/Evergreen minimum
BIOS Security	Please confirm that once an admin BIOS password is set, the BIOS should only be alterable with that password and through no other means or work around.
Network boot	The Device either has an inbuilt PXE compatible RJ45 socket or it must be possible to use a readily available PXE Compatible RJ45 to USB adapter with this model, please confirm.
Compliancy	Energy star certified or EPEAT
OEM Customer Specific Image Load Capability	Yes / No
DISM imaging possible	Yes / No
Image Configuration	Configured with a single image that can be used securely and safely ‘out of the box’?
Bulk Warranty Upload	Yes / No

Processor	Processor is at least Dual Core CPU minimum with Integrated Graphics, Capable of simultaneous moderate-intensity tasks and running the standard/curricular software
CPU benchmark	CPU benchmark of 2,200 for Windows laptops, see https://www.cpubenchmark.net/
Memory	Device has 4GB RAM or higher
Storage	Device has at least 64GB storage
Malware free	Confirm that devices will be supplied with a clean operating system with no malware or viruses
Drivers	All up-to-date drivers for Windows devices (laptops and tablets) submitted in tender responses must be available for download, by anyone, from the OEM website

Windows Tablets Device Minimum Specifications

Category	Device Requirement - Minimum Specification
Screen Size	10" or larger touch screen
Screen Resolution	HD (720 x 1280) or greater
Multimedia	Webcam VGA 640 x 480 minimum resolution
Connectivity	Wifi to 802.11ac minimum
Audio	Built in stereo speakers
Ports	Meets minimum specification of 2x USB 3.0 Type A sockets (and/or 1x USB 3.0 Type A socket and 1x USB 3.0 Type C socket)
Keyboard	Standard UK (detachable) keyboard included?
Audio Ports	Headphone/microphone socket – a single 3.5mm combined Headphone/Microphone jack required
Standard Warranty	Minimum 1-year warranty return to base as part of the tendered unit price.
Operating System	Minimum Windows 10 Professional Education version 2004 or 20H2 for devices available before October. S-mode not enabled.
Licences	Please confirm that the operating system license is included and pre-activated for standalone use and subsequent connection of the device to a school network/domain.

UK Language pack installed with Operating System	Yes / No
Recovery Partition Present	Yes / No
Bloatware	For devices being manufactured to order, please confirm that no bloatware will be present on the main or recovery partitions or if the device has already been manufactured please provide details in the table below.
Bluetooth	Bluetooth connection
Encryption	Bitlocker encryption as standard
Security Features	Please confirm (TPM 2.0 Minimum Requirement)
Battery	Integrated and non-detachable - Minimum 7 hours battery life.
PSU	Fitted with uk 3-pin as standard
S/W Image Consistency	12 Month Minimum
SCCM Support	Driver pack must be available - Please confirm
Autopilot	Is the Hardware Hash supplied in Intune compatible CSV format or is there an alternative mechanism that can be used by schools to generate this Hash on receipt of devices suppled to schools?
BIOS Update	UEFI/Evergreen minimum
BIOS Security	Once an admin BIOS password is set, the BIOS should only be alterable with that password and through no other means or work around.
Network boot	The Device either has an inbuilt PXE compatible RJ45 socket or it must be possible to use a readily available PXE Compatible RJ45 to USB adapters with this model, please confirm.
Compliancy	Energy star certified or EPEAT
OEM Customer Specific Image Load Capability	Yes / No
DISM imaging possible	Yes / No
Image Configuration	Configured with a single image that can be used securely and safely ‘out of the box’.
Bulk Warranty Upload	Yes / No
Sleeve Case	Are appropriately sized Sleeve Cases for these devices included within the unit cost?

Processor	Processor is at least Dual Core CPU minimum with Integrated Graphics, Capable of simultaneous moderate-intensity tasks and running the standard/curricular software
CPU benchmark	Device meets the minimum CPU benchmark of 1,500 for Windows Tablets, see https://www.cpubenchmark.net/
Memory	Device has at least 4GB RAM
Storage	Storage of 64GB or higher
Malware free	Confirm that devices will be supplied with a clean operating system with no malware or viruses
Drivers	All up-to-date drivers for Windows devices (laptops and tablets) submitted in tender responses must be available for download, by anyone, from the OEM website

Chromebooks Device Minimum Specifications

Category	Device Requirement - Minimum Specification
Screen Size	Device screen is 11" or larger
Screen Resolution	HD screen resolution is 720 x 1080 or greater
Multimedia	HD Webcam is 720p or greater
Connectivity	Wifi to 802.11ac minimum
Audio	Device has in-built speakers
Ports	Device includes 1 x USB 3.0 Type A socket and 1 x USB 3.0 Type C socket
Keyboard	Standard UK Keyboard included
Video Port	Does the device include a video port?
Audio Ports	Headphone/microphone socket – a single 3.5mm combined Headphone/Microphone jack required
Licences	Please confirm that Google Chrome Education Upgrade Licences have been included in the unit price submitted.
Standard Warranty	Minimum 1-year warranty return to base as part of the tendered unit price.
Operating System	ChromeOS with upgrade licence included in price
Bluetooth	Bluetooth connection
Device Encryption	Please confirm device encryption included
Memory	At least 4GB RAM
Processor	Processor is an Intel or AMD with Integrated Graphics or equivalent

Storage	16GB or more of storage
Battery	Integrated and non-detachable - Minimum 7 hours battery life, target 10 hours
PSU	Fitted with uk 3-pin as standard
Compliancy	Compliancy energy star certified or EPEAT
Bulk Warranty Upload	Yes / No

Ipads Device Minimum Specifications

Category	Device Requirement - Minimum Specification
Screen Size	Device screen size is at least 10.2"
Specification	7th or 8th generation Minimum - Please specify
Processor	Comes with apple A12 Bionic chip for 4k graphics?
Standard Warranty	Minimum 1-year warranty return to base as part of the tendered unit price.
PSU	Fitted with uk 3-pin as standard
Sleeve Case	Are Sleeve Cases for these devices included within the unit cost?

Android Device Minimum Specifications

Category	Device Requirement - Minimum Specification
Screen Size	Screen is at least 10" Touch screen
Screen Resolution	High definition resolution of at least 720x1280
Multimedia	Front and Rear facing cameras of at least 2.1mp – capable of 720p video resolution or better (front facing camera) usable in supplied sleeve/case
Connectivity	Wifi to 802.11ac minimum
Audio	Internal Speakers
Ports	1 x USB 2.0 Type A socket or 1 x USB 3.0 Type C
Keyboard	UK Standard on-screen Keyboard
Video/audio capture	Capable of capturing visual and audio content using inbuilt facilities
Audio Ports	Headphone/microphone socket – a single 3.5mm combined Headphone/Microphone jack
Standard Warranty	Minimum 1-year warranty return to base – manufacturer turnaround time to be outlined in the Price Schedule document

Operating System	Current Android Operating system with guaranteed android version updates and security updates for next 3 years
Bluetooth	Yes/No
Battery	Integrated and non-detachable - Minimum 7 hours battery life
PSU	Fitted with uk 3-pin as standard
Sleeve Case	Are Sleeve Cases for these devices included within the unit cost?
Processor	Dual core CPU minimum capable of simultaneous moderate-intensity tasks with evidence of successful use in the education sector.
Memory	2GB or more RAM
Storage	At least 32GB RAM minimum

Crown Commercial Service

ANNEX G: ONLINE ORDERING PLATFORM SECURITY REQUIREMENTS

i. The online ordering platform shall be:
   a. compliant with 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 and (where software-as-a-service is used to deliver components of the service) the NCSC SaaS Security Principles and accompanying guidance at https://www.ncsc.gov.uk/collection/saas-security/saas-security-principles
   b. compliant with the HMG Minimum Cyber Security Standards at https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
   c. securely implemented to ensure that it is not susceptible to the OWASP Top 10 Web Application Security Risks identified at https://owasp.org/www-project-top-ten/

ii. The Supplier shall comply with the Departmental Security Standards and Security Schedule as contained in the accompanying documents to this ITT.

iii. The Supplier shall undertake the departmental supplier security assurance process and undertake any resulting remediation activities identified by the Contracting Authority.

iv. The Supplier shall support the departmental security assurance process (DSAM) to which the service will be subject, by providing the required information about the technical and security implementation and operation of the ordering platform.

v. The Supplier shall only operate the online ordering platform once it has been granted an Authority to Operate (AtO) or otherwise directed by the Contracting Authority.

vi. The online ordering platform shall be configured with Multi Factor Authentication (MFA) for all access, including user access by schools, the Contracting Authority and Supplier personnel and privileged (administrator) access.

vii. The Supplier shall ensure that appropriate change management processes are in place for the online ordering platform and that any changes are reviewed by the Contracting Authority, to include security assessment, acceptance testing and authorisation.

viii. The Supplier shall undertake vulnerability assessments, including scanning, of the online ordering platform at a frequency of at least monthly, and report any identified vulnerabilities and weaknesses to the Contracting Authority.

ix. The Supplier shall apply security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as ‘Critical’ within 14 days of release, ‘Important’ within 30 days of release and all ‘Other’ within 60 days of release unless otherwise agreed with the Contracting Authority.

x. The Supplier shall ensure that access to the online ordering platform is by unique user identities and implemented on the basis of ‘least privilege’ where the minimum access privileges are assigned to fulfil particular roles and operations; this applies to both standard user and privileged (administrator) user access.

xi. All system administration of the online ordering platform shall be undertaken from an appropriately secured environment using an accountable authentication methodology.

xii. The Supplier shall ensure that development and testing environments are separated from the live systems.

xiii. Development and testing environments shall not contain live data.

xiv. The Supplier shall ensure that the online ordering platform is subject to an independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The ITHC shall include infrastructure, application, firewall and server configuration testing/reviews.

xv. The Supplier shall implement remediations against any vulnerabilities identified in the ITHC, as required by the Contracting Authority.

xvi. The Supplier shall provide the Contracting Authority with full details of any actual or future intent to develop, manage, support or operate the service, or store or access information relating to the service, outside of the UK mainland. The Supplier shall not go ahead with any such proposal without prior written agreement from the Contracting Authority.

xvii. The Supplier shall create and securely store security audit logs for the online ordering platform, which shall be retained for at least three months.

xviii. The Supplier shall ensure that security monitoring activities are undertaken to detect any attempted or actual security breaches of the online ordering platform.

xix. The Supplier shall ensure that Incidence Response and Recovery Plans, Business Continuity and Disaster Recovery plans are in place in case of a cyber-attack to ensure the availability of the ordering platform.

xx. On termination of the contract, the ordering platform shall be securely decommissioned. All data shall be securely transferred to the Contracting Authority and subsequently archived or deleted, as directed by the Authority.

Crown Commercial Service

DFE SECURITY CLAUSE

12. Departmental Security Standards for Business Services and ICT Contracts

"BPSS" "Baseline Personnel Security Standard"	means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"CPA" "Commercial Product Assurance" [formerly called "CESG Product Assurance"]	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body

“Data” “Data Controller” “Data Protection Officer” “Data Processor” “Personal Data” “Personal Data requiring Sensitive Processing” “Data Subject”, “Process” and “Processing”	shall have the meanings given to those terms by the Data Protection Act 2018
"Department’s Data" “Department’s Information”	is any data or information owned or retained in order to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Department is the Data Controller;
“DfE” “Department”	means the Department for Education
“Departmental Security Standards”	means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.
“Digital Marketplace / G-Cloud”	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
End User Devices	means the personal computer or consumer devices that store or process information.
“Good Industry Practice” “Industry Good Practice”	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.

“Good Industry Standard” “Industry Good Standard”	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
“GSC” “GSCP”	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
“HMG”	means Her Majesty’s Government
“ICT”	means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk

"OFFICIAL" "OFFICIAL-SENSITIVE"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP). the term 'OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.
"RBAC" "Role Based Access Control"	means Role Based Access Control. A method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"Secure Sanitisation"	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"Senior Information Risk Owner" "SIRO"	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SPF"	means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary

"HMG Security Policy Framework"	and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

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

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

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

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

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

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

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

12.7 The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.

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, application gateways, etc;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- use of secure device configuration and builds;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
- any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
    - retained and protected from tampering for a minimum period of six months;
    - made available to the department on request.

12.9 The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

12.10 The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.

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

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

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

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

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

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

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

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

Evidence of secure destruction will be required in all cases.

12.16 Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, 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. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, 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, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

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

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

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

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

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

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

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

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

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

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

Crown Commercial Service

BUYER ICT POLICY

(ICT Services)

1. Definitions

1.1. In this Schedule, the following words shall have the following meanings;

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

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

"Quality Plans"	has the meaning given to it in paragraph 6.1 of this Schedule;
"Sites"	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 9.1 of this Schedule;
"Source Code"	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
"Specially Written Software"	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
"Supplier System"	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

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

3. Buyer due diligence requirements

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

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

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

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

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

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

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

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

3.2.3. a timetable for and the costs of those actions.

4. Software warranty

4.1. The Supplier represents and warrants that:

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

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Supplier shall:

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

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

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

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

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

6. Standards and Quality Requirements

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

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

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

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

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

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

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

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

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

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

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

8. Maintenance of the ICT Environment

8.1. If specified by the Buyer undertaking a Further Competition, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("Maintenance Schedule") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer. In relation to this paragraph, the Supplier's ICT Environment comprises the Supplier systems used for the provision of the Deliverables including the following : REDACTED (Commercially Sensitive Information)

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

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

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

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

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

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

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

9.1.2. The Supplier shall:

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

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

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sublicense and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to

obtain the full benefits of ownership of the Specially Written Software and New IPRs.

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

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

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

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

b) third party software that is not COTS Software

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

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

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

9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

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

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

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

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

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

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

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

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

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

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

9.4.1.1. a Central Government Body; or

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

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

9.5. **Licence granted by the Buyer**

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

9.6. **Open Source Publication**

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

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

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

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

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

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

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

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

9.6.2.6. do not contain any Malicious Software.

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

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

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

9.7. **Malicious Software**

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

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

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

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the

Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

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

10. Supplier-Furnished Terms

10.1. Software Licence Terms

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

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

10.2. Software Support & Maintenance Terms

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

10.3. Software as a Service Terms

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

10.4. Device as a Service Terms

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

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

Clause 8.7

Clause 10.2

Clause 10.3.2]

11. CUSTOMER PREMISES – NOT APPLICABLE

ANNEX A TO BUYER ICT POLICY

Non-COTS Third Party Software Licensing Terms

The supplier shall provide details of all Non-COTS Third Party Software Licensing Terms within ten (10) working days of contract signature.

ANNEX B TO BUYER ICT POLICY

COTS Licensing Terms

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

ANNEX C TO BUYER ICT POLICY

Software Support & Maintenance Terms

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

ANNEX D TO BUYER ICT POLICY

Software as a Service Terms

Not in Use

ANNEX E TO BUYER ICT POLICY

Device as a Service Terms

Not in Use

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Supplier's Commercial Submission

REDACTED (Commercially Sensitive Information)

Invoicing

The Supplier shall invoice the Contracting Authority monthly in arrears according to the number of devices deployed within the period. The invoice proforma should be completed as agreed and accompany all invoices. The proforma should always show a clear and transparent connection between the devices volume, and the delivery and handling charges as a unit price per device received by the Services Partner for the scheme. Invoices submitted which are not in the prescribed format will not be accepted by the Contracting Authority.

INSERT WAVE AND PO NUMBER (IE: WAVE 8 CORE-PO-001234)											
Description	Quantity	Price	Invoice no' 11111111		Invoice no' 22222222		Total billed	Remaining	Total spend	Contract value	stock levels
			Volume	Invoice	Volume	Invoice					
Windows Devices											
IE: Dell Latitude 3190 Clamshell	10	£199.37	5	£996.85	2	£398.74	7	3	£1,395.59	£1,993.70	997
Chromebook Devices											
IE: Samsung Chromebook 4	20	£212.99	10	£2,129.90	0	£0.00	10	10	£2,129.90	£4,259.80	2130
TOTALS:	30	£412.36	15	£3,126.75	2	£398.74	17	13	£3,525.49	£6,253.50	3127

INVOICE NUMBER	QUANITY	VALUE	COMMENTS
11111111	15	£3,126.75	**Invoice paid.** Supplier will receive payment on 01/08/2021.
22222222	2	£398.74	**Invoice outstanding.** Currently at stage 1 financial assurance process.
	TOTAL SPEND SO F	£3,525.49	
	PO VALUE	##########	
	VARIANCE	##########	

Invoice is **paid** - this is signified by the

Invoice is **outstanding** - this is

How to complete this proforma:	
Column/cell	Action
Column A (Description)	Insert the product name as stated in the invoice
Column B (Quantity)	Insert the 'TOTAL' quantity as agreed in contract
Column C (Price)	Insert the 'UNIT' price as agreed in contract
Column D (Volume)	Insert the 'VOLUME/QUANTITY' as stated in the invoice
Columns H - K are contain formulas which are generate automa	
Column L	DfE to complete

Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables. Failure to invoice accurately, according to the agreed schedule shall incur penalties as set out at SLA 5 within the table at paragraph 15.6 of Attachment 4 in this Order Form.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

Invoices should be submitted to: Department for Education, 20 Great Smith Street, Westminster London, SW1P 3BT.

Part A – Milestone Payments and Delay Payments – Not Applicable

Part B – Service Charges – Not Applicable

Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges - Not Applicable

Part D – Risk Register – To Be Completed Post Contract Award within two weeks of Contract Commencement

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 12
Risk Number	Risk Name	Description of risk	Timing	Likelihood	Impact (£)	Impact (description)	Mitigation (description)	Cost of mitigation	Post-mitigation impact (£)	Owner

Part E – Early Termination Fee(s) - Not Applicable

Attachment 3 – Outline Implementation Plan

Implementation Plan, as co-Designed between the Buyer and Supplier, to be inserted within 20 days of Contract Commencement in line with Schedule 1 – Implementation Plan. The agreed Implementation Plan may lead to a re-baselining of the Services

Where the parties are required to complete and agree a deliverable within x working days of contract signature. Such deliverables will be agreed in accordance with the timescales set out in the Implementation Plan.

Please refer to Schedule 1 – Implementation Plan and Schedule 2 – Testing Procedures in Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses for full details.

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

Please refer to Service Levels and Service Credits Annex to be completed and agreed to by both parties within 10 working days of contract signature.

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
REDACTED (Personal Information)	REDACTED (Personal Information)	Entirety of Contract
REDACTED (Personal Information)	REDACTED (Personal Information)	Entirety of Contract

Part B – Key Sub-Contractors – Not Applicable

Attachment 6 – Software – Not Applicable

.1.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

.1.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software - Not Applicable

Part B – Third Party Software - Not Applicable

Attachment 7 – Financial Distress – To be completed post Contract Award by the Contracting Authority's Financial Business Partner

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

As part of due diligence, we are required to review all suppliers Financial Standing.
We would expect Bidders to be able to demonstrate a Financial Standing consistent with a D&B rating of 2 or lower.
We also reserve the right to request any further information required by the Financial Viability Risk Assessment Tool to undertake a further assessment of Financial Standing as required.
More information about how Government assesses Financial Standing is available from The Sourcing and Consultancy Playbook guidance for Assessment of Financial Standing

PART A – CREDIT RATING THRESHOLD

Entity	Credit Rating (long term)	Credit Rating Threshold
Computacenter (UK) Limited	**Dun & Bradstreet (requirement of a risk score of 2 or below)**	**Dun & Bradstreet – A risk score of 2 or below is normally required**

PART B – RATING AGENCIES

- [Rating Agency 1 (e.g Standard and Poors)]
  - Credit Rating Level 1 = [AAA]
  - Credit Rating Level 2 = [AA+]
  - Credit Rating Level 3 = [AA]
  - Credit Rating Level 4 = [AA-]
  - Credit Rating Level 5 = [A+]
  - Credit Rating Level 6 = [A]
  - Credit Rating Level 7 = [A-]
  - Credit Rating Level 8 = [BBB+]
  - Credit Rating Level 9 = [BBB]
  - Credit Rating Level 10 = [BBB-]
  - Etc.

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Contract Meetings	
Buyer Members for the Contract Meetings	REDACTED (Personal Information)
Supplier Members for the Operational Board	REDACTED (Personal Information)
Frequency of the Operational Board	Fortnightly
Location of the Operational Board	Virtual/Remote via Teams Invite

Operational Meetings	
Buyer Members for the Contract Meetings	REDACTED (Personal Information)
Supplier Members for the Operational Board	REDACTED (Personal Information)
Frequency of the Operational Board	Monday, Wednesday and Friday every week *frequency to be reviewed after 3 weeks
Location of the Operational Board	Virtual/Remote via Teams Invite

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 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 Schedule shall be with the Buyer at its absolute discretion.

- The contact details of the **Buyer's** Data Protection Officer are: REDACTED (Personal Information)
- The contact details of the **Supplier's** Data Protection Officer are:
- REDACTED (Personal Information)The Processor shall comply with any further written instructions with respect to processing by the Controller.
- Any such further instructions shall be incorporated into this Attachment 9.

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: • Business contact details of Supplier Personnel for which the Supplier is the Controller, • Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller. • Home address details of DfE employees, required for Supplier to ship test devices to.
Duration of the processing	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.
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.

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
Performance	Update reports on individual orders received and orders dispatched in a format as stated in section 8.1 in Statement of Requirements	Via a secure service to be agreed with the Contracting Authority	Daily
Charges	As per Attachment 2- Charges and Invoicing	Invoice Proforma Detailed listing of charges	Per Invoice
Performance management	Performance against SLA/KPI's	Contract Meetings: Powerpoint Slides to show performance against SLA/KPI's	Fortnightly

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

Schedule 1 - IMPLEMENTATION PLAN

S1 IMPLEMENTATION PLAN

1. INTRODUCTION

1.1 This Schedule S1 (Implementation Plan):

1.1.1 defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and

1.1.2 identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2. OUTLINE IMPLEMENTATION PLAN

2.1 The Outline Implementation Plan is set out in Attachment 3 (outline Implementation Plan) the Order Form.

2.2 All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 32 (Supplier Relief Due to Buyer Cause)).

3. APPROVAL OF THE DETAILED IMPLEMENTATION PLAN

3.1 The Supplier shall submit a draft of the Detailed Implementation Plan to the Buyer for approval within twenty (20) Working Days of the Commencement Date.

3.2 The Supplier shall ensure that the draft Detailed Implementation Plan:

3.2.1 incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan;

3.2.2 includes (as a minimum) the Supplier's proposed timescales in respect of the following for each of the Milestones:

(a) the completion of each design document;

(b) the completion of the build phase;

(c) the completion of any Testing to be undertaken in accordance with Schedule S2 (Testing Procedures); and

(d) training and roll-out activities;

3.2.3 clearly outlines all the steps required to implement the Milestones to be achieved in the next 15 months (or such other period agreed between the Parties), together with a high level plan for the rest of the programme;

3.2.4 clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and

3.2.5 is produced using a software tool as specified, or agreed by the Buyer.

3.3 Prior to the submission of the draft Detailed Implementation Plan to the Buyer in accordance with Paragraph **Error! Reference source not found.**, the Buyer shall have the right:

3.3.1 to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:

(a) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;

(e) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and

(f) any other work in progress in relation to the Detailed Implementation Plan; and

3.3.2 to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.

3.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Buyer shall:

3.4.1 review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and

3.4.2 notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than twenty (20) Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Buyer.

3.5 If the Buyer rejects the draft Detailed Implementation Plan:

3.5.1 the Buyer shall inform the Supplier in writing of its reasons for its rejection; and

3.5.2 the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Buyer's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Buyer for the Buyer's approval within twenty (20) Working Days of the date of the Buyer's notice of rejection. The provisions of Paragraph **Error! Reference source not found.** and this Paragraph **Error! Reference source not found.** shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3.6 If the Buyer approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Buyer’s notice of approval.

4. UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN

4.1 Following the approval of the Detailed Implementation Plan by the Buyer:

4.1.1 the Supplier shall submit a revised Detailed Implementation Plan to the Buyer every three (3) months starting three (3) months from the Commencement Date;

4.1.2 without prejudice to Paragraph **Error! Reference source not found.**, the Buyer shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Buyer within twenty (20) Working Days of receiving such a request from the Buyer (or such longer

period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);

4.1.3 any revised Detailed Implementation Plan shall (subject to Paragraph **Error! Reference source not found.**) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph **Error! Reference source not found.**; and

4.1.4 the Supplier's performance against the Implementation Plan shall be monitored at meetings of the Service Management Board (as defined in Part B of Schedule 7 (Governance) where used) or any such service management board established under Part A of Schedule 7 (Governance) where used. In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Buyer not less than five (5) Working Days in advance of such meeting.

4.2 Save for any amendments which are of a type identified and notified by the Buyer (at the Buyer's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:

4.2.1 any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and

4.2.2 in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 32 (Supplier Relief Due to Buyer Cause).

4.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Buyer.

5. GOVERNMENT REVIEWS

5.1 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

Schedule 2 - TESTING PROCEDURES

S2 TESTING PROCEDURES

DEFINITIONS

In this Schedule S2 (Testing Procedures), the following definitions shall apply:

"Component"	any constituent parts of the infrastructure for a Service, hardware or Software;
"Material Test Issue"	a Test Issue of Severity Level 1 or Severity Level 2;
"Severity Level"	the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Certificate"	a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable has satisfied its relevant Test Success Criteria;
"Test Issue"	any variance or non-conformity of a Deliverable from its requirements (such requirements being set out in the relevant Test Success Criteria);
"Test Issue Threshold"	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Issue Management Log"	a log for the recording of Test Issues as described further in Paragraph **Error! Reference source not found.**;
"Test Plan"	a plan: (a) for the Testing of Deliverables; and (b) setting out other agreed criteria related to the achievement of Milestones, as described further in Paragraph **Error! Reference source not found.**;
"Test Reports"	the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph **Error! Reference source not found.**;
"Test Strategy"	a strategy for the conduct of Testing as described further in Paragraph **Error! Reference source not found.**;
"Test Success Criteria"	in relation to a Test, the test success criteria for that Test as referred to in Paragraph **Error! Reference source not found.***;*
"Test Witness"	any person appointed by the Buyer pursuant to Paragraph **Error! Reference source not found.**; and
"Testing Procedures"	the applicable testing procedures and Test Success Criteria set out in this Schedule S2 (Testing Procedures).

1. RISK

1.1 The issue of a Test Certificate, a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not:

1.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or

1.1.2 affect the Buyer's right subsequently to reject:

(b) all or any element of the Deliverables to which a Test Certificate relates; or

(g) any Milestone to which the Milestone Achievement Certificate relates.

1.2 Notwithstanding the issuing of any Milestone Achievement Certificate, the Supplier shall remain solely responsible for ensuring that:

1.2.1 the Services are implemented in accordance with this Contract; and

1.2.2 each Service Level is met in accordance with this Contract.

2. TESTING OVERVIEW

2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, the Test Plans and the Test Specifications.

2.2 The Supplier shall not submit any Deliverable for Testing:

2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

2.2.2 until the Buyer has issued a Test Certificate in respect of any prior, dependant Deliverable(s); and

2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

2.4 Prior to the issue of a Test Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

2.5 Any Disputes between the Buyer and the Supplier regarding Testing shall be referred to the Dispute Resolution Procedure using the Expedited Dispute Timetable (as defined in Schedule 4 (Dispute Resolution Procedure) of this Contract).

3. TEST STRATEGY

3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Commencement Date but in any case no later than twenty (20) Working Days (or such other period as the Parties may agree in writing) after the Commencement Date.

3.2 The final Test Strategy shall include:

3.2.1 an overview of how Testing will be conducted in accordance with the Implementation Plan;

3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

3.2.3 the method for mapping the expected Test results to the Test Success Criteria;

3.2.4 the procedure to be followed if a Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issues;

3.2.5 the procedure to be followed to sign off each Test;

3.2.6 the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for the resolution of Test Issues;

3.2.7 the names and contact details of the Buyer's and the Supplier's Test representatives;

3.2.8 a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and Buyer and/or third party involvement in the conduct of the Tests;

(c) the technical environments required to support the Tests; and

(h) the procedure for managing the configuration of the Test environments.

4. TEST PLANS

4.1 The Supplier shall develop Test Plans and submit these for the approval of the Buyer as soon as practicable but in any case no later than twenty (20) Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start date for the relevant Testing (as specified in the Implementation Plan).

4.2 Each Test Plan shall include as a minimum:

4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being tested and, for each Test, the specific Test Success Criteria to be satisfied;

4.2.2 a detailed procedure for the Tests to be carried out, including:

(d) the timetable for the Tests, including start and end dates;

(i) the Testing mechanism;

(j) dates and methods by which the Buyer can inspect Test results or witness the Tests in order to establish that the Test Success Criteria have been met;

(k) the mechanism for ensuring the quality, completeness and relevance of the Tests;

(l) the format and an example of Test progress reports and the process with which the Buyer accesses daily Test schedules;

(m) the process which the Buyer will use to review Test Issues and the Supplier's progress in resolving these in a timely basis;

(n) the Test Schedule;

(o) the re-Test procedure, the timetable and the resources which would be required for re-Testing; and

(p) the process for escalating Test Issues from a re-test situation to the taking of specific remedial action to resolve the Test Issue.

4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plans provided that the Supplier shall incorporate any reasonable requirements of the Buyer in the Test Plans.

5. TEST SUCCESS CRITERIA

5.1 The Test Success Criteria for each Test that must be Achieved for the Supplier to Achieve a Milestone shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. TEST SPECIFICATION

6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least ten (10) Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise agree in writing) prior to the start of the relevant Testing (as specified in the Implementation Plan).

6.2 Each Test Specification shall include as a minimum:

6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4 Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

(e) a mechanism to be used to capture and record Test results; and

(q) a method to process the Test results to establish their content.

7. TESTING

7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may

be witnessed by the Test Witnesses in accordance with Paragraph **Error! Reference source not found.**.

7.3 The Supplier shall notify the Buyer at least ten (10) Working Days (or such other period as the Parties may agree in writing) in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests, except where the Buyer has specified in writing that such attendance is not necessary.

7.4 The Buyer may raise and close Test Issues during the Test witnessing process.

7.5 The Supplier shall provide to the Buyer in relation to each Test:

7.5.1 a draft Test Report not less than two (2) Working Days (or such other period as the Parties may agree in writing) prior to the date on which the Test is planned to end; and

7.5.2 the final Test Report within five (5) Working Days (or such other period as the Parties may agree in writing) of completion of Testing.

7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

7.6.1 an overview of the Testing conducted;

7.6.2 identification of the relevant Test Success Criteria that have been satisfied;

7.6.3 identification of the relevant Test Success Criteria that have not been satisfied together with the Supplier's explanation of why those criteria have not been met;

7.6.4 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

7.6.5 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph **Error! Reference source not found.**; and

7.6.6 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

8. TEST ISSUES

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute

Resolution Procedure using the Expedited Dispute Timetable (as defined in Schedule 4 (Dispute Resolution Procedure) of this Contract).

9. TEST WITNESSING

9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.3.7 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10. TEST QUALITY AUDIT

10.1 Without prejudice to its rights pursuant to Clause 29.2 (Records and Audit), the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

10.2 The focus of the Testing Quality Audits shall be on:

10.2.1 adherence to an agreed methodology;

10.2.2 adherence to the agreed Testing process;

10.2.3 adherence to the Quality Plan;

10.2.4 review of status and key development issues; and

10.2.5 identification of key risk areas.

10.3 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.4 The Buyer will give the Supplier at least five (5) Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit and the Supplier may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Supplier's reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Buyer will materially and adversely impact the Implementation Plan.

10.5 A Testing Quality Audit may involve document reviews, interviews with the Supplier Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule S2, the Buyer witnessing Tests and demonstrations of the Deliverables to the Buyer. Any Testing Quality Audit shall be limited in duration to a maximum time to be agreed between the Supplier and the Buyer on a case by case basis (such agreement not to be unreasonably withheld or delayed). The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.6 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall:

10.6.1 discuss the outcome of the Testing Quality Audit with the Supplier, giving the Supplier the opportunity to provide feedback in relation to specific activities; and

10.6.2 subsequently prepare a written report for the Supplier detailing its concerns,

and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

10.7 In the event of an inadequate response to the Buyer's report from the Supplier, the Buyer (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate) until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

11. OUTCOME OF TESTING

11.1 The Buyer shall issue a Test Certificate as soon as reasonably practicable when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

11.2.1 the Buyer may issue a Test Certificate conditional upon the remediation of the Test Issues;

11.2.2 where the Parties agree that there is sufficient time prior to the relevant Milestone Date, the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

12. ISSUE OF MILESTONE ACHIEVEMENT CERTIFICATE

12.1 The Buyer shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:

12.1.1 the issuing by the Buyer of Test Certificates and/or conditional Test Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

12.1.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone (which may include the submission of a Deliverable that is not due to be Tested, such as the production of Documentation).

12.2 The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Schedule 2 (Charges and Invoicing).

12.3 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out:

12.3.1 the applicable Test Issues ; and

12.3.2 any other reasons for the relevant Milestone not being Achieved.

12.4 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Milestone Achievement Certificate.

12.5 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Milestone Achievement Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

12.6 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Milestone Achievement Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

12.6.1 any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within ten (10) Working Days of receipt of the Buyer's report pursuant to Paragraph **Error! Reference source not found.**); and

12.6.2 where the Buyer issues a conditional Milestone Achievement Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

ANNEX 1: TEST ISSUES – SEVERITY LEVELS

.1 **Severity Level 1 Test Issue:** a Test Issue that causes non-recoverable conditions, e.g. it is not possible to continue using a Component, a Component crashes, there is database or file corruption, or data loss;

.2 **Severity Level 2 Test Issue:** a Test Issue for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

(a) causes a Component to become unusable;

(b) causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

(c) has an adverse impact on any other Component(s) or any other area of the Services;

.3 **Severity Level 3 Test Issue:** a Test Issue which:

(a) causes a Component to become unusable;

(b) causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

(c) has an impact on any other Component(s) or any other area of the Services; but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

.4 **Severity Level 4 Test Issue:** a Test Issue which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Services; and

.5 **Severity Level 5 Test Issue:** a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services

ANNEX 2: TEST CERTIFICATE

To: Computacenter (UK) Limited

FROM: Department for Education

[***Date***]

Dear Sirs,

TEST CERTIFICATE

Deliverables: [***insert description of Deliverables***]

We refer to the contract (the **"Contract"**) relating to the provision of the Services between the [***name of Buyer***] (the **"Buyer"**) and [***name of Supplier***] (the **"Supplier"**) dated [***date***].

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (Definitions) or Schedule S2 (Testing Procedures) of the Contract.

[We confirm that the Deliverables listed above have been tested successfully in accordance with the Test Plan relevant to those Deliverables.]

OR

[This Test Certificate is issued pursuant to Paragraph **Error! Reference source not found.** of Schedule S2 (Testing Procedures) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

**delete as appropriate*

Yours faithfully

[***Name***]

[***Position***]

acting on behalf of [***name of Buyer***]

ANNEX 3: MILESTONE ACHIEVEMENT CERTIFICATE

To: Computacenter (UK) Limited

FROM: Department for Education

[***Date***]

Dear Sirs,

MILESTONE ACHIEVEMENT CERTIFICATE

Milestone: [***insert description of Milestone***]

We refer to the contract (the **"Contract"**) relating to the provision of the Services between the [***name of Buyer***] (the **"Buyer"**) and [***name of Supplier***] (the **"Supplier"**) dated [***date***].

Capitalised terms used in this certificate have the meanings given to them in Schedule 1 (Definitions) or Schedule S2 (Testing Procedures) of the Contract.

[We confirm that all the Deliverables relating to Milestone [***number***] have been tested successfully in accordance with the Test Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]*

OR

[This Milestone Achievement Certificate is granted pursuant to Paragraph **Error! Reference source not found.** of Schedule S2 (Testing Procedures) of the Contract on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Schedule 2 (Charges and Invoicing)]*

**delete as appropriate*

Yours faithfully

[***Name***]

[***Position***]

acting on behalf of ***[name of Buyer***]

Schedule 3 - SECURITY REQUIREMENTS

S3 SECURITY REQUIREMENTS

PART A – SHORT FORM SECURITY REQUIREMENTS

1. DEFINITIONS

1.1 In this Part A of Schedule S3 (Security Requirements), the following definitions shall apply:

"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and is set out in the Order Form and as updated from time to time.

2. COMPLIANCE WITH SECURITY REQUIREMENTS AND UPDATES

2.1 The Supplier shall comply with the Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.2 Where the Security Policy applies, the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.3 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Services it may propose a Change to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be subject to the Change Control Procedure.

2.4 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Change Control Procedure the Supplier shall continue to provide the Services in accordance with its existing obligations.

3. SECURITY STANDARDS

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Services, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Services and/or the Buyer Data; and

3.2.4 where specified by the Buyer in accordance with Paragraph **Error! Reference source not found.** complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. SECURITY MANAGEMENT PLAN

Introduction

4.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Part A of Schedule S3 (Security Requirements). The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

Content of Security Management Plan

4.2 The Security Management Plan shall:

4.2.1 comply with the principles of security set out in Paragraph **Error! Reference source not found.** and any other provisions of this Contract relevant to security;

4.2.2 identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

4.2.3 detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Buyer with access to the Services, processes associated with the provision of the Services, the Buyer Premises, the Sites and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.4 be developed to protect all aspects of the Services and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.5 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Contract;

4.2.6 set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with Paragraph **Error! Reference source not found.** the Security Policy; and

4.2.7 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Services and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Part A Schedule S3 (Security Requirements).

Development of the Security Management Plan

4.3 Within twenty (20) Working Days after the Commencement Date and in accordance with Paragraph **Error! Reference source not found.**, the Supplier shall prepare and deliver to the Buyer for approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in the Order Form.

4.4 If the Security Management Plan submitted to the Buyer in accordance with Paragraph **Error! Reference source not found.**, or any subsequent revision to it in accordance with Paragraph **Error! Reference source not found.**, is approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Part A Schedule S3 (Security Requirements). If the Security Management Plan is not approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.5 The Buyer shall not unreasonably withhold or delay its decision to approve or not the Security Management Plan pursuant to Paragraph **Error! Reference source not found.**. However a refusal by the Buyer to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph **Error! Reference source not found.** shall be deemed to be reasonable.

4.6 Approval by the Buyer of the Security Management Plan pursuant to Paragraph **Error! Reference source not found.** or of any change to the Security Management Plan in accordance with Paragraph **Error! Reference source not found.** shall not relieve the Supplier of its obligations under this Part A Schedule S3 (Security Requirements).

Amendment of the Security Management Plan

4.7 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

4.7.1 emerging changes in Good Industry Practice;

4.7.2 any change or proposed change to the Services and/or associated processes;

4.7.3 where necessary in accordance with Paragraph **Error! Reference source not found.**, any change to the Security Policy;

4.7.4 any new perceived or changed security threats; and

4.7.5 any reasonable change in requirements requested by the Buyer.

4.8 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

4.8.1 suggested improvements to the effectiveness of the Security Management Plan;

4.8.2 updates to the risk assessments; and

4.8.3 suggested improvements in measuring the effectiveness of controls.

4.9 Subject to Paragraph **Error! Reference source not found.**, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph **Error! Reference source not found.**, a request by the Buyer or otherwise) shall be subject to the Change Control Procedure.

4.10 The Buyer may, acting reasonably, approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. SECURITY BREACH

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph **Error! Reference source not found.**, the Supplier shall:

5.3 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

5.3.1 minimise the extent of actual or potential harm caused by any Breach of Security;

5.3.2 remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

5.3.3 prevent an equivalent breach in the future exploiting the same cause failure; and

5.3.4 as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3.5 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with Paragraph **Error! Reference source not found.**) or the requirements of this Part A Schedule S3 (Security Requirements), then any required change to the Security Management Plan shall be at no cost to the Buyer.

Schedule 6 - BUSINESS CONTINUITY AND DISASTER RECOVERY

S6 BUSINESS CONTINUITY AND DISASTER RECOVERY

DEFINITIONS

1.1 In this Schedule, the following definitions shall apply:

"BCDR Plan"	has the meaning given to it in Paragraph **Error! Reference source not found.** of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph **Error! Reference source not found.** of this Schedule;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph **Error! Reference source not found.** of this Schedule;
"Related Supplier"	any person who provides services to the Buyer which are related to the Services from time to time;
"Review Report"	has the meaning given to it in Paragraph **Error! Reference source not found.** of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph **Error! Reference source not found.** of this Schedule;

2. BCDR PLAN

2.1 At least five (5) Working Days prior to the Commencement Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

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

2.1.2 the recovery of the Services in the event of a Disaster

2.2 The BCDR Plan shall be divided into three sections:

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

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

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

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

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

3.1 Section 1 of the BCDR Plan shall:

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

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

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

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

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

3.1.6 contain a risk analysis, including:

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

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

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

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

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

3.1.8 set out key contact details for the Supplier (and any Sub-Contractors) and for the Buyer;

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

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

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

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

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

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

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

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

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

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

3.4 The Supplier shall not be entitled to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. BUSINESS CONTINUITY (SECTION 2)

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

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

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

4.2 The Business Continuity Plan shall:

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

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

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

5. DISASTER RECOVERY (SECTION 3)

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

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

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

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

5.2.4 loss of a Sub-Contractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

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

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

5.2.12 testing and management arrangements.

6. REVIEW AND CHANGING THE BCDR PLAN

6.1 The Supplier shall review the BCDR Plan:

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

6.1.2 within three (3) calendar months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph **Error! Reference source not found.**; and

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

6.2 Each review of the BCDR Plan pursuant to Paragraph **Error! Reference source not found.** shall assess its suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

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

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

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

7. TESTING THE BCDR PLAN

7.1 The Supplier shall test the BCDR Plan:

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

7.1.2 in the event of any major reconfiguration of the Services; and

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

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

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

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

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

7.5.1 the outcome of the test;

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

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

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

8. INVOKING THE BCDR PLAN

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

Schedule 7 - CONTINUOUS IMPROVEMENT

S7 CONTINUOUS IMPROVEMENT

1. SUPPLIER'S OBLIGATIONS

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

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

1.3 NOT APPLICABLE

1.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for approval within six (6) Months following the Commencement Date, whichever is earlier.

1.5 The Buyer shall notify the Supplier of its approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

1.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

1.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Change in accordance with the Change Control Procedure and the Supplier must implement such Change at no additional cost to the Buyer.

1.8 Once the first Continuous Improvement Plan has been approved in accordance with Paragraph **Error! Reference source not found.**:

1.8.1 the Supplier shall use all reasonable endeavours to implement any agreed services in accordance with the Continuous Improvement Plan; and

1.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

1.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph **Error! Reference source not found.**.

1.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

1.11 Should the Supplier's costs in providing the Services to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Services.

1.12 At any time during the Contract Period of this Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.