Direct award Order Form Template

CALL-OFF REFERENCE:	**Project_5104**
THE BUYER:	**The Secretary of State for Education whose acting as part of the Crown ("the Department", "The Customer")**
BUYER ADDRESS:	**Sanctuary Buildings, Great Smith Street, London, SW1P 3BT**
SUPPLIER REFERENCE	RM3808-Covid-Lot 1-Abzorb Group Ltd – FILTEREDSIMS-10122020
THE SUPPLIER:	Abzorb Group Ltd
SUPPLIER ADDRESS:	Armytage Road, Brighouse, West Yorkshire, HD6 1QF
REGISTRATION NUMBER:	10779280
DUNS NUMBER:	222979503
SID4GOV ID:	**n/a**

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 11/12/2020
It is issued under the Framework Contract with the reference number RM3808 for the provision of Network Services.

CALL-OFF LOT(S):
Lot 1 Data Access Services & Lot 6 Mobile Voice and Data Services

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

1. This Order Form including the Call-Off Special Terms and Call-Off special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM3808
3. The following Schedules in equal order of precedence:

   Joint Schedules for framework reference number RM3808

- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)

- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data) as amended and set out in this agreement

Schedules for this Contract

- Call Off Schedule 1 (Security)
- Call Off Schedule 2 (Prices)
- Call Off Schedule 3 (Call Off Specification)
- Call Off Schedule 4 (Service Levels)

4. CCS Core Terms (version 3.0.5)
5. Joint Schedule 5 (Corporate Social Responsibility)

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

CALL-OFF SPECIAL TERMS
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

CALL-OFF START DATE n/a

CALL-OFF EXPIRY DATE n/a

CALL-OFF INITIAL PERIOD n/a

CALL-OFF OPTIONAL EXTENSION PERIOD n/a

MINIMUM PERIOD OF NOTICE FOR WITHOUT REASON TERMINATION

90 days

CATALOGUE SERVICE OFFER REFERENCE: RM3808-Covid-Lot 1-Abzorb Group Ltd – FILTEREDSIMS

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 3 (Call-Off Specification)

DELIVERY LOCATION
REDACTED

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

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is REDACTED

CALL-OFF CHARGES

See details in Call-Off Schedule 2 (Pricing Details)

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4 and 5 in Framework Schedule 3 (Framework Prices).

The Charges will not be impacted by any change to the Framework Prices.

REIMBURSABLE EXPENSES
Not recoverable

BACs – via PO

BUYER'S INVOICE ADDRESS:
Department for Education
Sanctuary Buildings
20 Great Smith Street
London
SW1P 3BT

BUYER'S AUTHORISED REPRESENTATIVE
REDACTED

ADDITIONAL INSURANCES
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

GUARANTEE
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

QUALITY PLAN
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

MAINTENANCE OF ICT ENVIRONMENT
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

BUYER'S SECURITY POLICY
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

SUPPLIER'S AUTHORISED REPRESENTATIVE
REDACTED

SUPPLIER'S CONTRACT MANAGER
REDACTED

OPERATIONAL BOARD
Not applicable when the Call-Off Contract is awarded through a direct award procedure.

COMMERCIALLY SENSITIVE INFORMATION
[Not applicable]

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

SCHEDULE 11

Joint Schedule 11 – Processing Data

Status of the Controller

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

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

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

11.1.1.3 "Joint Controller" with the other Party;

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

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

Where one Party is Controller and the other Party its Processor

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

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

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

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

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

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

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

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

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

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

11.1.5.2.1 nature of the data to be protected;

11.1.5.2.2 harm that might result from a Data Loss Event;

11.1.5.2.3 state of technological development; and

11.1.5.2.4 cost of implementing any measures;

11.1.5.3 ensure that :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11.1.6.6 becomes aware of a Data Loss Event.

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

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

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

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

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

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

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

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

11.1.9.1 the Controller determines that the Processing is not occasional;

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

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

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

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

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

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

11.1.12.2 obtain the written consent of the Controller;

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

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

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

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

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

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix 1

Processing Personal Data

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

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

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

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

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

Personal Data Processing Template

Description	**Details**
Identity of Controller for each Category of Personal Data	The Relevant Authority is Controller and the Supplier is Processor. The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: (a) The information relating to the Responsible Bodies **The Relevant Authority is a joint controller with the Responsible Bodies and the Supplier is the Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority and the Responsible Bodies are Joint Data Controller and the Supplier is the Processor of the following Personal Data: (a) The collection of data to allow web filtering on the of devices (b) Data used to support the execution of the contract (c) Data used to capture an audit trail of activity (d) Data used to resolve any delivery or ordering dispute issues **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: (a) Business contact details of Supplier Personnel for which the Supplier is the Controller

	(b) Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller.
Duration of the Processing	12 months from contract signature.
Nature and purposes of the Processing	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose includes the ordering, setup, management, and updating of the devices, this includes monitoring usage, making security changes and locating the device in the event of loss.
Type of Personal Data	The Authority and the Responsible Bodies will require the following data: (a) Name of student, and asset number associated with the device (b) Location of device (c) Online history (d) The Processor will require the following data (e) Administrator email address, first and last name as well as Billing contact name are stored within the platform. (f) Roaming Client Hostname (g) External and Internal IP addresses (h) Destination URL (i) Timestamp *Cisco will process all personal data in accordance with their published privacy notices* - https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/security/umbrella-privacy-data-sheet.pdf
Categories of Data Subject	Responsible bodies and their staff (including volunteers, agents, and temporary workers), and name of individuals who are allocated devices.
Plan for return and destruction of the data once the Processing is complete **UNLESS requirement under Union or Member State law to preserve that type of data**	Data would need to be held for 7 (seven) years for statutory financial purposes.

Framework Contract Personal Data Processing

Description	Details
Identity of Controller for each Category of Personal Data	DfE is Controller and the Supplier is Processor. The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 and for the purposes of the Data Protection Legislation, DfE is the Controller and the Supplier is the Processor of the Personal Data recorded below
Duration of the Processing	Up to 7 (seven) years after the expiry or termination of the Framework Contract.
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this Framework Contract including: (a) Ensuring effective communication between the Supplier and CSS (b) Maintaining full and accurate records of every Call-Off Contract arising under the Framework Agreement in accordance with Core Terms Clause 15 (Record Keeping and Reporting)
Type of Personal Data	Includes: (a) Contact details of, and communications with, CSS staff concerned with management of the Framework Contract (b) Contact details of, and communications with, Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract, (c) Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract Contact details, and communications with Supplier staff concerned with management of the Framework Contract
Categories of Data Subject	Includes: (a) CSS staff concerned with management of the Framework Contract (b) Buyer staff concerned with award and management of Call-Off Contracts awarded under the Framework Contract (c) Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this Framework Contract Supplier staff concerned with fulfilment of the Supplier's obligations arising under this Framework Contract

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**	All relevant data to be deleted 7(seven) years after the expiry or termination of this Framework Contract unless longer retention is required by Law or the terms of any Call-Off Contract arising hereunder.

JOINT SCHEDULE 11

Joint Controller Agreement

1. **Joint Controller Status and Allocation of Responsibilities**

11.1.1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Law in respect of their Processing of such Personal Data as Data Controllers.

11.1.1.2 The Parties agree that the applicable Responsible Bodies

11.1.1.2.1 is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

11.1.1.2.2 shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

11.1.1.2.3 is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

11.1.1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

11.1.1.2.5 shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the applicable responsible privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

11.1.1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. **Undertakings of both Parties**

11.1.2.1 The Supplier and the Relevant Authority each undertake that they shall:

11.1.2.1.1 report to the other Party every 6 months on:

(a) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(b) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(c) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(d) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(e) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

11.1.2.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in paragraphs 2.1(a)(i) to (v);

11.1.2.1.3 provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in paragraphs 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

11.1.2.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under the Contract or is required by Law, to be notified to the other Party. For the avoidance of doubt any third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

11.1.2.1.5 request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

11.1.2.1.6 ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

11.1.2.1.7 take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(a) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(b) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so;

(c) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation ;

11.1.2.1.8 ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

11.1.2.1.9 ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation , to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

11.1.2.1.10 ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

11.1.2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. **Data Protection Breach**

11.1.3.1 Without prejudice to paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the Relevant Authority and its advisors with:

11.1.3.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

11.1.3.1.2 all reasonable assistance, including:

(a) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(b) co-operation with the other Party including taking such reasonable steps as are directed by the Relevant Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(c) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(d) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

11.1.3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has been lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach with information relating to the Personal Data Breach, in particular:

11.1.3.2.1 the nature of the Personal Data Breach;

11.1.3.2.2 the nature of Personal Data affected;

11.1.3.2.3 the categories and number of Data Subjects concerned;

11.1.3.2.4 the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

11.1.3.2.5 measures taken or proposed to be taken to address the Personal Data Breach; and

11.1.3.2.6 describe the likely consequences of the Personal Data Breach.

4. **Audit**

11.1.4.1 The Supplier shall permit:

11.1.4.1.1 the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits,

assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation ; and/or

11.1.4.1.2 the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

11.1.4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **Impact Assessments**

11.1.5.1 The Parties shall:

11.1.5.1.1 provide all reasonable assistance to the each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

11.1.5.1.2 maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

6. **ICO Guidance**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. **Liabilities for Data Protection Breach**

11.1.7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

11.1.7.1.1 if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

11.1.7.1.2 if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

11.1.7.1.3 if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

11.1.7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

11.1.7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

11.1.7.3.1 if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

11.1.7.3.2 if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

11.1.7.3.3 if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

11.1.7.4 Nothing in either paragraph If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court. or paragraph In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"): shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. **Termination**

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 (*Ending the contract*).

9. **Sub-Processing**

11.1.9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

11.1.9.1.1 carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

11.1.9.1.2 ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation .

10. **Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

CALL OFF SCHEDULE 1 - SECURITY

Commodity Service Security Requirements

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

   - the Departmental Security Requirements (Annex 1)

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

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

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

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

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

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

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

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

ANNEX 1

1. **Departmental Security Requirements**

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**	shall have the meanings given to those terms by the Data Protection Act 2018

Processing	
Buyer's Data **Buyer'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 Supplier by or Buyer; or (ii) (which the Supplier 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 **Buyer**	means the Department for Education
Departmental Security Standards	means the Buyer's security policy or any standards, procedures, process or specification for security that the Supplier 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	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP).
OFFICIAL-SENSITIVE	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 (ie disks or virtual disks) over a network interface rather than using physically connected storage.
Secure Sanitisation	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

	The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
Security and Information Risk Advisor **CCP SIRA** **SIRA**	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
Senior Information Risk Owner **SIRO**	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms-length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
SPF **HMG Security Policy Framework**	means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

4.1.1.1 HMG security policy framework, NCSC guidelines and where applicable DfE Departmental Security Standards for Suppliers which include but are not constrained to the following clauses.

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

4.1.1.3 Where clause 1.2 above has not been met, the Supplier 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 Buyer. 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).

4.1.1.4 The Supplier 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 Supplier has an existing Protective Marking Scheme then the Supplier 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).

4.1.1.5 Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Supplier's or Subcontractor'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 1.14.

4.1.1.6 The Supplier 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.

4.1.1.7 The Supplier 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).

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

4.1.1.8.1 physical security controls;

4.1.1.8.2 good industry standard policies and processes;

4.1.1.8.3 malware protection;

4.1.1.8.4 boundary access controls including firewalls;

4.1.1.8.5 maintenance and use of fully supported software packages in accordance with vendor recommendations;

4.1.1.8.6 software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

4.1.1.8.7 user access controls, and;

4.1.1.8.8 the creation and retention of audit logs of system, application and security events.

4.1.1.9 The Supplier 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.

4.1.1.10 The Supplier 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 Buyer except where the department has given its prior written consent to an alternative arrangement.

4.1.1.11 The Supplier 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.

4.1.1.12 Whilst in the Supplier'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".

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

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

4.1.1.14 In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier’s assets and must be returned to the Buyer 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 1.15.

4.1.1.15 In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier 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 Supplier or sub-Supplier shall protect the Buyer’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.

4.1.1.16 Access by the Supplier or Subcontractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Buyer. All Supplier or Subcontractor staff must complete this process before access to Departmental Data is permitted.

4.1.1.17 All Supplier or Subcontractor employees who handle Departmental Data shall have annual awareness training in protecting information.

4.1.1.18 The Supplier 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 Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

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

Incidents shall be reported to the Buyer 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 Supplier 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 Supplier with outcomes being notified to the Buyer.

4.1.1.20 The Supplier 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 Buyer and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

4.1.1.21 The Supplier or Subcontractors 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 Supplier or Subcontractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.

4.1.1.22 The Buyer reserves the right to audit the Supplier or Subcontractors 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 Supplier's, and any Subcontractors', compliance with the clauses contained in this Section.

4.1.1.23 The Supplier and Subcontractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the Buyer. This will include obtaining any necessary professional security resources required to support the Supplier's and Subcontractor'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.

4.1.1.24 Where the Supplier is delivering an ICT solution to the Buyer 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 Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer's expectation is that the Supplier shall provide written evidence of:

4.1.1.24.1 Compliance with HMG Minimum Cyber Security Standard.

4.1.1.24.2 Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.

4.1.1.24.3 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.

4.1.1.24.4 Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Supplier shall provide details of who the awarding body or organisation will be and date expected.

4.1.1.25 The Supplier shall contractually enforce all these Departmental Security Standards for Suppliers onto any third-party suppliers, Subcontractors or partners who could potentially access Departmental Data in the course of providing this service.

Call Off Schedule 2 – Prices

1. Charges

1.1 The price for the connectivity and associated services is:

Charge Component	Per User, per month
5000 x 2GB per SIM data (aggregated across the estate) from the date falling 48 hours following the dispatch of the relevant Roaming SIM Card to the School or Social Care Body	REDACTED

1.2 The price for configuration and associated services is:

Charge Component	Price
Configuration of 5000 routers	REDACTED
Delivery of 1 batch to single location	REDACTED
Delivery of 3 batches to single location	REDACTED

1.3 Optional additional charges not included within 1.1. These will be ordered via a separate purchase order as and when required and include the charges for increasing the data should the aggregate data cap be insufficient.

Charge Component		Charge (per user)
Change requested to all SIMs, prior to the beginning of the month. Applied to the all SIMs in time for the beginning of the month.	3GB Data per user, per month	REDACTED
	4GB Data per user, per month	REDACTED
	5GB Data per user, per month	REDACTED
	20GB Data per user, per month	REDACTED
Blocks 1 TB of data added to total data pool, before the current month has ended.		REDACTED
Excess Data Charge per MB, should individual users have their cap lifted and the data pool is exceeded, without adding additional bundles (in line with the above) prior to the pool being breached		REDACTED
Replacement SIM		REDACTED

(a) No additional Charges will be payable in respect of data usage where the applicable aggregate data cap at the relevant time has not been exceeded.

(a) INVOICING

(b) The Supplier will invoice the Buyer monthly in advance in respect of line rental charges (1.1). Any SIMs dispatched and activated in the preceding month, will incur a pro-rata charge for the time connected.

(c) Data Roaming usage will commence forty-eight (48) hours after the despatch of each device/SIM to the school or social care setting.

1.3.2 4G SIM Requirements

(a) 4G/LTE SIM installed into Mifi Device or e-SIM configured

(b) Data only Roaming SIM Card, no voice or text allowance

(c) Minimum 2GB monthly allowance per Roaming SIM Card/MiFi Device

(d) Pooled data allowance with detailed real-time reporting, split by Responsible Body and MiFi Device

(e) Data pool to be combined with Wave 1 data pool, to allow all users from both contracts to access the same allowance of data.

(f) Pre-agreed means of adding additional data

(g) UK Data roaming included to allow connection to other providers in areas of low/poor signal

1.3.3 Filtering Requirement

(a) ISP-level filtering service (as set out below) with customisable whitelists/blacklists by Buyer. Changes to be agreed between all parties in advance. Such agreement not to be unreasonably withheld by the Supplier.

(b) The Supplier shall procure that its communication service provider must support DNS filtering solutions provisioned on Buyer connected devices and shall not in any way prejudice the efficacy of the DNS filtering solution.

(c) The Internet Watch Foundation (IWF) Child Abuse Image Content List as updated and made available shall be implemented promptly on the service.

(d) The filtering service must not impair the need to comply with the requirements set out in Keeping Children Safe in Education (KCSIE) 2019 document and referenced PREVENT duty guidance as updated April 2019.

(e) In line with the Buyer's statutory guidance set out in the KCSIE guidance, internet content filtering must be in place to prevent children from accessing illegal and inappropriate internet content and to ensure children are safe from terrorist and extremist material.

(f) Measures in place to prevent access to illegal internet content, specifically:

(i) A content filtering system that subscribes to IWF (Internet Watch Foundation) block list of illegal Child Sexual Abuse Material (CSAM)

(ii) Integrate the ‘the police assessed list of unlawful terrorist content, produced on behalf of The Home Office.

1.3.4 Data Protection

(a) To the extent that the Supplier receives Personal Data, it shall comply with the requirements of Joint Schedule 11 (Data Protection).

(b) In all cases, the Supplier should not be sent (and will not accept) any data that could become Personal Data including but not limited to a student's name, their school, home address, contact details.

(c) For the purposes of this Agreement, the Supplier will simply assign a SIM card with its own generated IP address and record details of the SIM card. It has no purpose nor need to perform its obligations under the Agreement for any other data that could lead to it becoming Personal Data in relation to a student/end user.

1.3.5 Inappropriate Online Content

Filtering must prevent access to the following categories of inappropriate internet content within the constraints of Internet Service Provider filtering:

(i) Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010

(ii) Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances

(iii) Extremism: promotes terrorism and terrorist ideologies, violence or intolerance

(iv) Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

(v) Pornography: displays sexual acts or explicit images

(vi) Piracy and copyright theft: includes illegal provision of copyrighted material

(vii) Self-Harm: promotes or displays deliberate self-harm (including suicide and eating disorders)

(viii) Violence: Displays or promotes the use of physical force intended to hurt or kill.

(b) This list should not be considered exhaustive and the Supplier shall produce on this content.

Call Off Schedule 4 – Service Levels

Section 1 - Definitions

In this Call Off Schedule 4, the following words shall have the following meanings

Critical Service Failure	means a failure to meet a Service Level Threshold in respect of a Service Level as set out below;
Service Level Failure	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
Service Level Performance Measure	shall be as set out against the relevant Service Level in the Annex to this Schedule 4;
Service Level Threshold	shall be as set out against the relevant Service Level in the Annex to to this Schedule 4;
Service Period	a period of one month commencing on the date upon which the first MiFi Devices are shipped to the School or Social Care Body and each subsequent month thereafter;
Mobile Phone Operator	the operator of the Network to which a SIM Card is connected;
Network	the third party Mobile Device digital network over which the Services are provided;
4G Service Availability	the service availability dictated by the individual availability, capacity and network coverage of the mobile phone operators. The Roaming SIM Cards that provide the connectivity, will authenticate on to any one of the 4 UK mobile phone operators, impartially. This means it will provide an equivalent service to any SIM card locked to one network, on any of the networks it connects to.

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

14.1.1.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in this Schedule 4.

(b) CRITICAL SERVICE LEVEL FAILURE

14.1.1.3 A Critical Service Level Failure will be deemed to have occurred where the Supplier has breached the Critical Service Level failure threshold Table 1A.

14.1.1.4 The Buyer shall be entitled to apply Service Credits where the Supplier fails to meet the Critical Service Level failure threshold as per Table 1A .

14.1.1.5 For each Critical Service Level failure the associated Service Credit shall be calculated as set out in Table 1A and shall be deducted from the invoice for the immediately following month provided that in the sixth month following the date upon which the first MiFi Devices are shipped to the School or Social Care Body, any applicable Service Credits shall be deducted from the Charges for that month.

Section 2: Service Levels

1. SERVICE LEVELS

14.1.1.1 If the level of performance of the Supplier is likely to or fails to meet any Service Level Threshold as detailed this shall be reported in accordance with Section 4 of this Schedule. Following notification by the Supplier to the Buyer, the Buyer, in its absolute discretion and without limiting any other of its rights, may

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

14.1.1.1.2 instruct the Supplier to comply with the Rectification Plan Process:

(a) for the Critical Service Levels failures as set out in Table 1A

(b) for all other Service Level failures, where the number of failures of a Service Level have exceeded the number set out against such Service Level in Table 1B

14.1.1.1.3 if a Critical Service Level Failure has occurred, exercise its right to Service Credits in accordance with Section 1.

1A – CRITICAL SERVICE LEVELS

Service Level Performance Criterion	Key Indicator	Critical Service Level Performance Target	Critical Service Level failure threshold (Number of Service Level Failures to trigger Service Credit and requirement for a Rectification Plan)	Service Credit % Payable
4G Service Availability	Availability	4G Service Availability will be no worse than would be the availability of a SIM card locked to the highest available network provider	One failure affecting 25% or more of the Roaming SIM Cards in use for a period greater than 1 hr duration per month, in two consecutive months	£9833 per month

Service Level Performance Criterion	Key Indicator	Critical Service Level Performance Target	Critical Service Level failure threshold (Number of Service Level Failures to trigger Service Credit and requirement for a Rectification Plan)	Service Credit % Payable
Red Flag Issues	Block SIM	100% within 4hr at all times	Two failures in one month	£9833 per month

1B – OTHER SERVICE LEVELS

Service Level Performance Criterion	Key Indicator	Service Level Performance Target	Service Level failure threshold (Number of Service Level Failures to trigger requirement for a Rectification Plan)

Lost/Stolen device	Block SIM	Within 4 business hours	5 failures in 1 month subject to Support Provision in Annex 1 (subject to a maximum of 500 requests per week)
Data Cap Reached	Resolution of tickets that are related to the data allowance.	By the end of the next business day.	5 failures in 1 month subject to Support Provision in Annex 1 (subject to a maximum of 150 requests per week)

ANNEX 1: SUPPORT PROVISION

1st Line Support – Responsible Bodies (RBs)	
Supplier In-Life Service Support	
Hours of Operation: • Red Flag Issues	Monday to Sunday 24hrs
Device/SIM – Lost or Stolen	Responsible Bodies to Log lost or stolen Router and/or SIM via support portal.

	Supplier to resolve tickets that relate to service disabling requests within 4 business hours, blocking the SIM immediately and informing the responsible body.
Data Cap Reached	Management of Data Cap. 20GB is a hard cap. Any user hitting the data per month allocation will have the service disabled for the rest of the calendar month. This may be increased on a per user basis, based upon shared capacity in the aggregated data pool. This will be handled on a manual basis via the support portal. Supplier to resolve tickets that are related to the data allowance by the end of the next business day.
Red Flag Issues	Issues related to the safety and wellbeing of a young person. (e.g. such as access to inappropriate material taking place). Resolve tickets that are related in any way related to the safety and wellbeing of a young person within 4 hours of a Red Flag request being logged on the support portal.
4G & Filtering support	
Web Filtering	Ensure that all content filtering services described in Schedule 3 (Specification) are maintained up to date with the latest watchlist information available from IWF and the Home Office. Support removal of agreed whitelisted sites from data caps/allowances.