Direct award Order Form Template

CALL-OFF REFERENCE:	Project_5166
THE BUYER:	**The Secretary of State for Education whose acting as part of the Crown ("the Department", "The Customer", "The Authority")**
BUYER ADDRESS:	**Sanctuary Buildings, Great Smith Street, London, SW1P 3BT**
SUPPLIER REFERENCE	RM3808-Covid-Lot 1-Abzorb Group Ltd – FILTEREDSIMS-13012021
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 13th January 2021.
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

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)

- Call-Off Schedules
  - Call-Off Schedule 5 (Pricing Details)
  - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 10 (Exit Management)
  - Call-Off Schedule 14 (Service Levels)
  - Call-Off Schedule 20 (Call-Off Specification)

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 13th January 2021

CALL-OFF EXPIRY DATE 31st July 2021

CALL-OFF INITIAL PERIOD 6 Months

CALL-OFF OPTIONAL EXTENSION PERIOD 12 Months

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 20 (Call-Off Specification)

DELIVERY LOCATION

REDACTED

MAXIMUM LIABILITY

REDACTED

CALL-OFF CHARGES
See details in Call-Off Schedule 5 (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

PAYMENT METHOD

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

BUYER'S INVOICE ADDRESS:

REDACTED

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED

BUYER'S ENVIRONMENTAL POLICY
Not applicable

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.

SOCIAL VALUE COMMITMENT
Not applicable

STAFF TRANSFER
Not applicable

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.

BUSINESS CONTINUITY AND DISASTER RECOVERY
In accordance with Call-Off Schedule 8 (Business Continuity and Disaster Recovery) Part A, the Supplier's BCDR Plan REDACTED.

SECURITY REQUIREMENTS
In accordance with Call-Off Schedule 9, Part A (Short Form Security Requirements) and Annex A: Department for Education additional security clauses to apply.

BUYER'S SECURITY POLICY
In accordance with Annex A: Department for Education of this Call Off Order Form.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)
A bespoke ISMS option is not available when the Call-Off Contract is awarded through a direct award procedure.

CLUSTERING
Not Applicable

SERVICE LEVELS AND SERVICE CREDITS
As described in Schedule 14

The Service Period is one (1) Month

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.

KEY STAFF
Not Applicable

KEY SUBCONTRACTOR(S)
Not Applicable

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	REDACTED	Signature:	REDACTED
Name:	REDACTED	Name:	REDACTED
Role:		Role:	
Date:	13.01.2021	Date:	13.01.2021

Annex A: Departmental Security Requirements

Definitions:

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

Personal Data	
Personal Data requiring Sensitive Processing	
Data Subject	
Process and	
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 data-base 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	means the Department for Education
Buyer	
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 frame-work 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

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.

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.

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. 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).

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.

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.

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).

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:

8.1 physical security controls;

8.2. good industry standard policies and processes;

8.3. malware protection;

8.4. boundary access controls including firewalls;

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

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

8.7 user access controls, and;

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

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.

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.

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.

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".

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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:

    24.1 Compliance with HMG Minimum Cyber Security Standard.

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

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.

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.

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.

Joint Schedule 11 (Processing Data)

1.1 The only processing that the Processor is authorised to do is listed in this Joint Schedule11 by the Controller and may not be determined by the Processor.

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

1.3 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:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Deliverables;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

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

1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

(a) process that Personal Data only in accordance with this Joint Schedule 11(Processing 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;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, 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:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular this Joint Schedule 11 (Processing Data);

(ii) 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 clause;

(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 this Contract; and

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

(d) 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:

(i) 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;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) 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

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(e) 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.

1.5 Subject to paragraph 1.6, the Processor shall notify the Controller immediately if it:

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

(b) receives a request to rectify, block or erase any Personal Data;

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

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;

(e) 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

(f) becomes aware of a Data Loss Event.

1.6 The Processor's obligation to notify under paragraph 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

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

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

(d) assistance as requested by the Controller following any Data Loss Event;

(e) 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.

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

(a) the Controller determines that the processing is not occasional;

(b) 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

(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Joint Schedule 11 (Processing Data) such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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 this Contract).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 Where the Parties include two or more Joint Controllers as identified in in this Joint Schedule 11 (Processing Data) (in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Annex 2 in replacement of paragraphs 1.1-1.14 for the Personal Data under Joint Control.

Annex 1 (Joint Schedule 11) Authorised Processing Personal Data

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
Categories of Da-	Responsible bodies and their staff (including volunteers, agents, and temporary workers), and name of individuals who are allocated

ta Subject	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.

Call Off Schedule 5 – Pricing

1. Charges

1.1 The total price for the connectivity and associated services is: £739,382.58

Charge Component	Per User, per month
REDACTED	REDACTED
REDACTED	

1.2 The price for configuration and associated services is:

Charge Component	Price
REDACTED	REDACTED
REDACTED	REDACTED
REDACTED	REDACTED

1.3 REDACTED.

Charge Component		Charge (per user)
REDACTED	REDACTED	REDACTED
	REDACTED	REDACTED
	REDACTED	REDACTED
	REDACTED	REDACTED
REDACTED		REDACTED
REDACTED		REDACTED
REDACTED		REDACTED

(a) REDACTED

1.4 INVOICING

(a) The Supplier will invoice the Buyer REDACTED.

(b) Data Roaming usage will commence REDACTED.

Schedule 14 – Service Levels & Service Credits

Section 1 - Definitions

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

Critical Service Failure	means a failure to meet a Service Level Threshold in respect of a Service Level 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 14;
Service Level Threshold	shall be as set out against the relevant Service Level in the Annex to this Schedule 14;
Service Period	a period of one month commencing on REDACTED;
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. REDACTED.

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

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

2. Critical Service Level Failure

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

2.2. 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 .

2.3. For each Critical Service Level failure the associated Service Credit shall be calculated as REDACTED

3. SERVICE LEVELS

3.1. 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 14 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

- require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer;
- instruct the Supplier to comply with the Rectification Plan Process:
- for the Critical Service Levels failures as set out in Table 1A

3.2. 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

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

CRITICAL SERVICE LEVELS

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

OTHER SERVICE LEVELS

REDACTED	REDACTED	REDACTED	REDACTED

REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

ANNEX 1: REDACTED

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

Call Off Schedule 20 – Specification

1. 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

2 Filtering Requirement

(a) ISP-level filtering service (as set out below) with customisable white-lists/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:

- A content filtering system that subscribes to IWF (Internet Watch Foundation) block list of illegal Child Sexual Abuse Material (CSAM)
- Integrate the ‘the police assessed list of unlawful terrorist content, produced on behalf of The Home Office.

3 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.

4 Inappropriate Online Content

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

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

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

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

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

(e) Pornography: displays sexual acts or explicit images

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

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

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

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

5 Configuration

5.1 Configuration of the MiFi device, including but not limited to:

(a) unboxing the mifi
(b) putting the SIM into the mifi
(c) updating the settings on the mifi

(d) reboxing the MiFi with on the box / in the box information
(e) where there's a failed configuration, record failure
(f) validate internet and device to laptop connectivity

5.2 Reporting:

(a) numbers of device configured per day
(b) number DOA MiFi devices
(c) number and % of failed configuration attempts
(d) serial / IMEI number to SIM card to understand which router is with which SIM and to enable end to end support linking mifi to sim to RB

5.3 Logistics

(a) Logistics reporting (inbound and outbound) between suppliers
(b) Logistics to enable configuration: