BUYER REFERENCE Connectivity – Project_4335

This Agreement is made on the 7th day of May 2020 between

(1) **The Secretary Of State For Education** of Sanctuary Buildings, 20 Great Smith Street, London SW1P 3BT (**the Buyer**)

(2) **Computacenter (UK) Limited** (registered in England and Wales under number 01584718) whose registered office is at Hatfield Avenue, Hatfield AL10 9TW (**the Supplier**)

RECITALS

(A) This Contract relates to the provision of deliverables and various associated services by the Supplier to the Buyer.

(B) The parties have agreed to base this Contract on the contractual structure set out in Framework Contract RM6068 for the provision of Technology Products and Associated Services but this Contract is not an award by the Buyer under that Framework Contract.

NOW IT IS HEREBY AGREED AS FOLLOWS:

1. INTERPRETATION

1.1 In this Contract, the following words shall have the following meanings and they shall supplement the defined terms contained in Joint Schedule 1 (Definitions):

REDACTED	**REDACTED**
Contract	this agreement including all the terms incorporated from RM6068, and only the Joint Schedules and the Schedules as specified in Clause 1.2 below. No other schedules shall apply to this agreement;
Dead on Arrival" or "DoA	the relevant MiFi Device appears undamaged after shipping but fails to operate after power-on when received by the School or Social Care Body;
Devices	the laptop and tablet device to be supplied by the Supplier under the Devices Contract;
Devices Contract	the contract dated 19 April 2020 entered into between the Buyer and the Supplier in relation to the supply of Devices;
Expiry Date	the date of the last to expire of the warranties in relation to the Deliverables;
Helpdesk	an additional telephone call back service available to support the Responsible Body. Helpdesk Service Support Hours will be managed through to resolution during the hours 09.00 – 17.00 Hours, Monday to Friday, excluding Bank Holidays.
Image Build	a standard off the shelf Windows 10 Professional EDU operating system provided by Microsoft where some additional software and configuration items have been overlaid;
In-Life Service	the support service in respect of the MiFi Devices and the SIM Cards to be provided by the Supplier following the deployment of

	such items to the Schools and the Social Care Bodies as more particularly set out in Annex B of Schedule 20 (Specification);
Initial Period	the period commencing on the Start Date and ending on the date which falls six (6) months following the date that the last of the MiFi Devices have been shipped by the Supplier to the School or Social Care Body;
Internet Watch Foundation or IWF	the Internet Watch Foundation of Discovery House, Vision Park, Chivers Way, Histon, Cambridge CB24 9ZR;
REDACTED	**REDACTED**
Longstop Date	30 June 2020;
MiFi Devices	the wireless routers that act as mobile Wi-Fi hotspots forming part of the Deliverables to be delivered by the Supplier to the Schools and the Social Care Bodies;
Nominated Support Contacts	individuals at Responsible Bodies who have been nominated as authorised users of the Support Portal;
Red Flag Issues	incidents which are in any way related to a young person being able to access a website(s) that should otherwise be blocked by the filtering requirements set out in paragraph 3 of Annex A of Schedule 20 (Specification);
Red Flag Issues Tickets	tickets raised through the Support Portal relating to Red Flag Issues;
Responsible Bodies	Local Authorities, Multi Academy Trusts and Social Care Bodies;
Roaming SIM Cards	the SIM cards which form part of the Deliverables and which are to be inserted by the Supplier into the MiFi Devices and delivered by the Supplier to the Schools and Social Care Bodies;
School	an educational establishment to which Deliverables will be dispatched by the Supplier;
Social Care Body	a social care organisation to which Deliverables will be dispatched by the Supplier;
Secondary Period	the period from the end of the Initial Period until the date falling twenty four (24) months following the date of issue of the last MiFi Device to a School or Social Care Body;
Start Date	7 May 2020;
Schools/Social Care Bodies	the delivery locations for MiFi Devices and accountable for liaising with end users;
Support Portal	the online portal available 24x7 for Nominated Support Contacts at Responsible Bodies to initiate support requests;
REDACTED	**REDACTED**
Term	the Initial Period and the Second Period unless this Contract is terminated earlier in accordance with its terms;

REDACTED **REDACTED**

1.2 The following documents are incorporated into this Contract. Where numbers are missing, the relevant schedules are not incorporated into this Contract. If the documents conflict, the following order of precedence applies:

1.2.1 This agreement including the Special Terms and Schedules.

1.2.2 Joint Schedule 1 (Definitions and Interpretation) RM6068

1.2.3 The following Schedules in equal order of precedence:

Joint Schedules for RM6068:

(a) Joint Schedule 2 (Variation Form)

(b) Joint Schedule 3 (Insurance Requirements)

(c) Joint Schedule 4 (Commercially Sensitive Information)

(d) Joint Schedule 6 (Key Subcontractors)

(e) Joint Schedule 10 (Rectification Plan)

(f) Joint Schedule 11 (Processing Data) as amended and set out in this agreement

Schedules for this Contract:

(a) Schedule 1 (Transparency Reports)

(b) Schedule 5 (Pricing Details)

(c) Schedule 6 (ICT Services)

(d) Schedule 8 (Business Continuity & Disaster Recovery)

(e) Schedule 9 (Security)

(f) Schedule 10 (Exit Management)

(g) Schedule 13 (Implementation Plan and Testing)

(h) Schedule 14 (Service Levels)

(i) Schedule 15 (Call-Off Contract Management)

(j) Schedule 20 (Call-Off Specification)

1.2.4 Core Terms (version 3.0.6) ("**Core Terms**") as amended by Clause 2.1

1.2.5 Annexes A to E Schedule 6 (ICT Services)

1.3 No other Supplier terms are part of this Contract. That includes any terms presented at the time of delivery.

2. SPECIAL TERMS

2.1 The Core Terms shall be amended as follows:

2.1.1 To the extent that is required to give effect to the incorporation of the Core Terms into this Contract, the Buyer shall be deemed to be CCS in all of the relevant Core Terms and the Supplier acknowledges and agrees that the Buyer shall be entitled to enforce those relevant Core Terms as if it were CCS.

2.1.2 **REDACTED**

2.2 The following Special Terms are incorporated into this Contract:

Special Term 1: REDACTED

Special Term 2: REDACTED

Special Term 3: REDACTED

Special Term 4: REDACTED

Special Term 5: REDACTED

Special Term 6: REDACTED

Special Term 7: REDACTED

Special Term 8: REDACTED

Special Term 9: REDACTED

Special Term 10: REDACTED

Special Term 11:

Modern Slavery, Child Labour and Inhumane Treatment

1.1 The Supplier:

1.1.1 shall not use, or allow its Subcontractors to use, forced, bonded or involuntary prison labour;

1.1.2 shall not require any Supplier staff or Subcontractor staff to lodge deposits or identity papers with the Employer or deny Supplier staff freedom to leave their employer after reasonable notice;

1.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;

1.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world;

1.1.5 shall make reasonable enquiries to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world;

1.1.6 shall have and maintain throughout the Term of the Call-Off Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and shall include in its contracts with its subcontractors anti-slavery and human trafficking provisions;

1.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under this Call-Off Contract;

1.1.8 shall prepare and deliver to the Buyer within fourteen (14) days of the Start Date and updated on a frequency defined by the Department, a slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business;

1.1.9 shall not use, or allow its employees or Subcontractors to use, physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

1.1.10 shall not use, or allow its Subcontractors to use, child or slave labour;

1.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to the Buyer and Modern Slavery Helpline1.

3. DELIVERABLES

3.1 The details of the Deliverables to be supplied by the Supplier are set out in Schedule 20 (Call-Off Specification).

3.2 The Supplier shall deliver the Deliverables to the Schools and the Social Care Bodies. The delivery addresses for the schools shall be as agreed in the order for the devices in the Devices Contract and for Social Care will be the single location notified by the Social Care contact in a pre-ordering telephone call.

3.3 The details relating to the delivery dates of the Deliverables are set out in Schedule 13 (Implementation Plan & Testing)

3.4 The provisions relating to the testing of Deliverables are contained in Call-Off Schedule 13 (Implementation Plan & Testing)

4. WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be the duration of any guarantee or warranty period the Supplier has received from the third party manufacturer or supplier.

5. MAXIMUM LIABILITY

REDACTED

6. CHARGES

6.1 The details of the Charges are contained in Schedule 5 (Pricing Details)

6.2 The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law.

[1] The "Modern Slavery Helpline" refers to the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

6.3 There are no Reimbursable Expenses

7. PAYMENT METHOD

7.1 The Buyer's Invoice Address is:

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

7.2 The Buyer's Authorised Representative is:

REDACTED

REDACTED

REDACTED

8. BUYER'S SECURITY POLICY

The details of the Buyer's Security Policy are contained in Schedule 9 (Security).

9. SUPPLIER'S AUTHORISED REPRESENTATIVE

9.1 The Supplier's Authorised Representative is:

REDACTED

REDACTED

REDACTED

9.2 The Supplier's Contract Manager is:

REDACTED

REDACTED

REDACTED

10. PROGRESS REPORT FREQUENCY

The details of the report frequency are contained in Schedule 1 (Transparency Reports)

11. PROGRESS MEETING FREQUENCY

The details of the progress meeting frequency are set out in Schedule 15 (Call-Off Contract Management)

12. KEY SUBCONTRACTOR(S)

REDACTED

13. COMMERCIALLY SENSITIVE INFORMATION

The details of the Supplier's Commercially Sensitive Information are contained in Joint Schedule 4 (Commercially Sensitive Information)

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

SCHEDULE 4

Joint Schedule 4 – Commercially Sensitive Information

1. WHAT IS THE COMMERCIALLY SENSITIVE INFORMATION?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
	7 May 2020	Special Terms	Term + 2 years
		Clause 1.1 – definitions of subcontractors	
		Clauses 5, 7.2, 9 and 12	
		Joint Schedule 3 – Insurance Requirements	
		Paragraphs 1.1, 1.2, 1.3, 2.1, 2.2, 2.3, 3.1, Annex A and Annex B of Schedule 5 (Pricing Details)	
		Schedule 1 – references to (REDACTED) and (REDACTED)	
		Schedule 8 (BCDR)	
		Part 2 of Schedule 13 (Implementation Plan and Testing)	
		Schedule 14 (Service Levels)	
		Schedule 20 (Specification) – Annex B and Buyer Dependencies in Annex C	

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:

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

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

1.3 "Joint Controller" with the other Party;

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

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

Where one Party is Controller and the other Party its Processor

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

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

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

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

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

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

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

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

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

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

5.2.1 nature of the data to be protected;

5.2.2 harm that might result from a Data Loss Event;

5.2.3 state of technological development; and

5.2.4 cost of implementing any measures;

5.3 ensure that :

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

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

(a) are aware of and comply 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;

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

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

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

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

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

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

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

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

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

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

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

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

6.6 becomes aware of a Data Loss Event.

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

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

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

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

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

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

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

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

9.1 the Controller determines that the Processing is not occasional;

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

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

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

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

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

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

12.2 obtain the written consent of the Controller;

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

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

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

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

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

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

32. 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.

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.

Appendix 2

Joint Controller Agreement

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

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.

1.2 The Parties agree that the applicable Responsible Bodies

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;

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;

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;

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

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).

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**

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

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;

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);

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;

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;

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;

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;

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 ;

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;

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

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

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**

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:

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;

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.

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:

3.2.1 the nature of the Personal Data Breach;

3.2.2 the nature of Personal Data affected;

3.2.3 the categories and number of Data Subjects concerned;

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;

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

3.2.6 describe the likely consequences of the Personal Data Breach.

4. **Audit**

4.1 The Supplier shall permit:

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

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.

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**

5.1 The Parties shall:

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

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**

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:

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;

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

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*).

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.

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"):

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;

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

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.

7.4 Nothing in either paragraph 7.2 of **Error! Reference source not found.** or paragraph 7.3 of **Error! Reference source not found.** 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**

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

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

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.

SCHEDULE 1

Call-Off Schedule 1 – Transparency Reports

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

1.2 Within ten (10) days of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

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

ANNEX A

List of Transparency Reports

It is key to the Buyer that regular reporting as set out below is adhered to. The principles that the Buyer and the Supplier have agreed in relation to the key data required to demonstrate the performance of the Supplier is based on the following principles:

1. Responsible Bodies will have access to the ordering portal (**REDACTED**) to monitor the progress of their orders through the supply chain. It is not expected that the Buyer will use the portal for reporting and that the Supplier will run Transparency Reports directly from the portal and other systems internally and issue formatted reports accordingly as set out below. The Supplier must ensure that the reporting is clearly split to show the following two separate groups:

1.1 Responsible Bodies (including Local Authorities acting in their role as a Responsible Body for a School)

1.2 Local Authorities social care team (prefixed with a code sc)

Title	Content	Format	Freq.	Content Provided	Produced By:	Buyer Contact
Performance - Summary report by Responsible Body on its position in the process.	To include as a minimum open for ordering, vendor type, orders placed, orders fulfilled	Excel	Daily	To include as a minimum - Survey completed - forecast captured - cap approved - open for ordering - vendor type - orders placed - orders fulfilled	Supplier	**REDACTED**
Performance – Responsible Body level of data usage	Daily report of usage of all units in use in terms of data used as % of maximum allowance broken down by Responsible Body to The Buyer	Support Portal	Daily	- Responsible Body ID - Total Data Used Across RB (GB) - Number of Live Connections within RB - Average Data Usage per Connection (GB) - Aggregated Allowance (GB) - RB Allowance Utilisation (%) - Average Utilisation per Connection (%)- Itemised list of SIM numbers, actual data usage within period, % usage of monthly allowance, and status (showing for example whether blocked and reason)	Supplier **(REDACTED)**	Nominated Buyer contact(s)
Performance – Units in service and blocked	Provide daily report to the Buyer of number and % of units in service, number of units blocked from use for reaching data cap, number of units blocked due to theft or other intervention, overall and broken down by Responsible Body.	Support Portal	Daily	- Responsible Body ID - Number of Live Connections within RB - Number of Connections Reached Data Cap - Number of Data Caps Released - Number of SIM Cards Manually Barred (Month to Date)	Supplier **(REDACTED)**	Nominated Buyer contact(s)
Performance – Units active and inactive	Provide daily report to the Buyer of number and % of units that have been issued that are activated, that are issued but not yet activated	Support Portal	Daily	- Responsible Body ID - Number of Live Connections within RB - Number of Connections in Use - Number of Connections with	Supplier **(REDACTED)**	Nominated Buyer contact(s)

Title	Content	Format	Freq.	Content Provided	Produced By:	Buyer Contact
	and that are issued but currently blocked, overall and by Responsible Body.			Zero Usage (Connection Date to Date) - Number of SIM Cards Barred / Data Capped		
Performance – Reports for Responsible Bodies	Distribute daily report for each Responsible Body, listing Roaming SIM Card numbers, actual data usage within the period, % usage of the monthly allowance and status (showing for example whether blocked and reason).	Support Portal	Daily	Responsible Body ID SIM Numbers Actual data usage within period % usage of monthly data allowance Status (showing for example whether blocked and reason)	Supplier **(REDACTED)**	
Performance – Data contracts	Provide a weekly report itemising data bundles providing details of start and end dates to the Buyer	Support Portal	Weekly	- Responsible Body ID - Number of Connections Activated on W1 (Start date of XXX / End date of XXX) - Number of Connections Activated on W2 (Start date of XXX / End date of XXX) - Number of Connections Activated on W3 (Start date of XXX / End date of XXX) - Number of Connections Activated on W4 (Start date of XXX / End date of XXX) - Number of Connections Activated on W5 (Start date of XXX / End date of XXX) - Number of Connections Activated on W6 (Start date of XXX / End date of XXX) - Number of Connections Activated on W7 (Start date of XXX / End date of XXX)	Supplier **(REDACTED)**	Nominated Buyer contact(s)
Performance – Helpdesk performance	Provide weekly report to the Buyer to provide an overview of the use of the helpdesk service showing performance against each of the following categories. Report should itemise the source, nature of the incident, action taken, time taken to inform the Responsible Body and time taken to resolve: Tickets that are related to a young person being unable to access service when they are within the data allowance for their device Red Flag Issue Tickets (As per Schedule 20 – Specification, Red Flag Tickets are for incidents which are in any way related to a young person being able to access a website(s) that should be otherwise be blocked by the filtering requirement (Section 3 of Schedule 20). Theft Tickets	Support Portal	Weekly	- Service Now Report Can be sent - Detail on no access to service can be provided. Where this is caused from areas of no service this cannot be reported. - Red Flag Tickets Reports will be added on a daily basis - Lost/Stolen Statistics can be provided - Ticket Type overview can be provided relating to data allowance transfer requests - Number of web queries can be reported on - Number of calls handled can be included	Supplier **(REDACTED)**	Nominated Buyer contact(s)

Title	Content	Format	Freq.	Content Provided	Produced By:	Buyer Contact
	Tickets that are related to the transfer of data allowance between users from Responsible Bodies Report also to include: Number of web queries submitted. Number of calls handled					
Performance – Red Flag Issues and Theft Tickets	Provide the Buyer with a daily report on Red Flag Issues and theft tickets (as described in Schedule 20 - Specification). Itemising the source, nature of the incident, action taken and time taken to inform Responsible Body and time taken resolve.	Support Portal	Daily	- Stolen Tickets can be provided in a Service now Report - Report should split out : 1 reconfiguration w/ warranty numbers 2. Lost and stolen	Supplier **(REDACTED)**	Nominated Buyer contact(s)
Performance – Filtering Services	Provide the Buyer with a daily report on content filtering services described in Annex A of Schedule 20 (Specification). Report should be itemised by filtering service and confirm they are maintained up to date with the latest watchlist information available from IWF and the Home Office.	Support Portal	Daily	- The latest versions of the IWF and CITRU list are always available. These are updated in line with the latest versions from the appropriate bodies. - Reports will also include attempted access detail	Supplier **(REDACTED)**	Nominated Buyer contact(s)
Performance - Daily "outstanding orders" report	List of live approved orders by Responsible Body showing order status of deliveries	Excel	Daily	List of live approved orders by Responsible Body showing order status of deliveries	Supplier	**REDACTED**
Performance – Orders completed	List of completed orders by Responsible Body	Excel	Daily	List of completed orders by Responsible Body including device breakdown and quantity	Supplier	**REDACTED**
Technical – ordering portal performance and support team	To include a daily report of ordering portal uptime and outages and daily volumes of Responsible Body inquiry presented and answered	Excel	Weekly	To include a daily report of portal uptime and outages and daily volumes of Responsible Body inquiry presented and answered	Supplier	**REDACTED**
DOA Reports	List of DOA MiFi Devices by delivery location and action taken	Excel	Weekly	Serial Number Delivery Location Date Action Taken	Supplier	**REDACTED**
MiFi Device serial number and SIM serial number	List of MiFi Device and Roaming SIM Card serial numbers by delivery location	Excel	Despatch + 1	Delivery location MiFi Device serial number Roaming SIM Card serial number	Supplier	**REDACTED**

Where appropriate a single merged report covering the above reporting requirements and the reporting requirements of the Devices Contract will be produced

SCHEDULE 5

Call off – Pricing Details

1. CHARGES

1.1 REDACTED

1.2 REDACTED

1.3 REDACTED

1.4 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.

2. INVOICING

2.1 REDACTED

2.2 REDACTED

2.3 REDACTED

2.4 Data Roaming usage will commence forty-eight (48) hours after the despatch of each device/SIM to the School or Social Care Body.

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

3. ASSUMPTIONS

3.1 REDACTED

3.2 In the event that any one or more of the Assumptions set out in paragraph 3.1 proves to be incorrect or where they change then the parties shall work together (acting reasonably and in good faith) to reduce the impact of this within the agreed timescales and estimated Charges and failing that then either:

3.2.1 The parties shall agree a Variation to deal with the impact; or

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

4. ADDITIONAL INFORMATION

DESCRIPTION	INCLUDED IN CHARGES?
Travel and expenses	N/A
VAT	Excluded
Any duties or levies other than value added tax	Excluded
Packaging, packing, shipping, carriage, insurance and delivery of Deliverables to the Delivery Address	Included
Warranty	• 24-month manufacturer warranty on MiFi Device included • 6-month manufacturer warranty on MiFi Device battery included

DESCRIPTION	INCLUDED IN CHARGES?
	• Web Filtering warranty Excluded
Configuration	• Recording of MiFi Device serial number included • Recording of Roaming SIM Card serial number included • Asset label applied to MiFi Device included • Powering on/off of MiFi Device for DOA test included
SIM Lock	• (REDACTED) to remotely lock Roaming Sim Card to MiFi Device prior to MiFi Device being shipped to delivery location

ANNEX A

REDACTED

ANNEX B

BUY AND STORE OR CUSTOMER OWNED KIT AGREEMENT

REDACTED

SCHEDULE 6

ICT Services

1. DEFINITIONS

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

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

ICT Environment	the Buyer System and the Supplier System;
Licensed Software	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
Malicious Software	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
New Release	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
Open Source Software	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;
Operating Environment	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: (a) the Deliverables are (or are to be) provided; or (b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or (c) where any part of the Supplier System is situated;
Quality Plans	has the meaning given to it in Paragraph 5.1 of **Error! Reference source not found. Error! Reference source not found.**of this Schedule;
Sites	has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;
Software	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
Software Supporting Materials	has the meaning given to it in Paragraph 7.1 of **Error! Reference source not found.** of this Schedule;
Source Code	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and

	documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
Specially Written Software	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;
Supplier System	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. WHEN THIS SCHEDULE SHOULD BE USED

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

3. SOFTWARE WARRANTY

3.1 The Supplier represents and warrants that:

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

3.1.2 all components of the Specially Written Software shall:

(a) be free from material design and programming errors;

(b) perform in all material respects in accordance with the relevant specifications and Documentation; and

(c) not infringe any IPR.

4. PROVISION OF ICT SERVICES

4.1 The Supplier shall:

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

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

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

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

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

5. STANDARDS AND QUALITY REQUIREMENTS

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

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

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

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

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

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

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

6. ICT AUDIT

6.1 The Supplier shall allow any auditor access to the Supplier premises to:

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

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

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

7. INTELLECTUAL PROPERTY RIGHTS IN ICT

7.1 Assignments granted by the Supplier: Specially Written Software

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

(a) the Documentation, Source Code and the Object Code of the Specially Written Software; and

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

7.1.2 The Supplier shall:

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

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

(c) without prejudice to paragraph 7.1.2(b), provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

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

7.2 Licences for non-COTS IPR from the Supplier and third parties to the Buyer

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

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

(b) third party software that is not COTS Software

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

7.2.3 Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 7.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

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

(b) only use such third party IPR as referred to at paragraph 7.2.3(a) if the Buyer Approves the terms of the licence from the relevant third party.

7.2.4 Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 7.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

7.2.5 The Supplier may terminate a licence granted under Paragraph 7.2.2 of **Error! Reference source not found.** by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

7.3 Licenses for COTS Software by the Supplier and third parties to the Buyer

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

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

7.3.3 Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 7.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

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

(a) will no longer be maintained or supported by the developer; or

(b) will no longer be made commercially available

7.4 Buyer's right to assign/novate licences

7.4.1 The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 9.2 of **Error! Reference source not found.** (to:

(a) a Central Government Body; or

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

7.4.2 If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in Paragraph 7.2 of **Error! Reference source not found.**.

7.5 Licence granted by the Buyer

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

7.6 Open Source Publication

7.6.1 Unless the Buyer otherwise agrees in advance in writing (and subject to Paragraph 7.6.3 of **Error! Reference source not found.** all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

(a) suitable for publication by the Buyer as Open Source; and

(b) based on Open Standards (where applicable),

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

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

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

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

(c) do not contain any material which would bring the Buyer into disrepute;

(d) can be published as Open Source without breaching the rights of any third party;

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

(f) do not contain any Malicious Software.

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

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

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

7.7 Malicious Software

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

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

7.7.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 7.7.2 of **Error! Reference source not found.** shall be borne by the Parties as follows:

(a) by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

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

8. SUPPLIER-FURNISHED TERMS

8.1 Software Licence Terms

8.1.1 Terms for licensing of non-COTS third party software in accordance with Paragraph 7.2.3 are detailed in Annex A of this Call-Off Schedule 6.

8.1.2 Terms for licensing of COTS software in accordance with Paragraph 7.3 are detailed in Annex B of this Call-Off Schedule 6.

8.2 Software Support & Maintenance Terms

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

8.3 Software as a Service Terms

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

8.4 Device as a Service Terms

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

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

Clause 6.7;

Clause 8.2;

Clause 8.3.2.

9. CUSTOMER PREMISES

9.1 Licence to occupy Customer Premises

9.1.1 Any Customer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Call- Off Contract. The Supplier shall have the use of such Customer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Call-Off Contract and in accordance with Call-Off Schedule 10 (Exit Management).

9.1.2 The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Call-Off Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

9.1.3 Should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this paragraph 9.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

9.1.4 The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

9.1.5 The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Call-Off Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

9.2 Security of Buyer Premises

9.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

9.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

10. BUYER PROPERTY

10.1 Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

10.2 The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

10.3 The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

10.4 The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

10.5 The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with this Call-Off Contract and for no other purpose without Approval.

10.6 The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance with Call- Off Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

10.7 The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by a Buyer Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

11. SUPPLIER EQUIPMENT

11.1 Unless otherwise stated in this Call Off Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

11.2 The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

11.3 The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Call-Off Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

11.4 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

11.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Call Off Contract, including the Service Levels.

11.6 The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

11.7 The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

11.7.1 remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with this Call-Off Contract; and

11.7.2 replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

APPENDIX 3

Non-COTS Third Party Software Licensing Terms

The Supplier shall provide details of all Non-COTS Third Party Software Licensing Terms within ten (10) Working Days of contract signature

APPENDIX 4

COTS Licensing Terms

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

APPENDIX 5

Software Support & Maintenance Terms

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

APPENDIX 6

Software as a Service Terms

N/A

APPENDIX 7

Device as a Service Terms

N/A

SCHEDULE 8

Business Continuity and Disaster Recovery

REDACTED

ANNEX 1

Supplier's Business Continuity and Disaster Recovery Policy Statement

REDACTED

ANNEX 2

REDACTED

ANNEX 3

REDACTED

SCHEDULE 9

Call off – 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

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.

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.

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).

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).

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.

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.

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).

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:

1.8.1 physical security controls;

1.8.2 good industry standard policies and processes;

1.8.3 malware protection;

1.8.4 boundary access controls including firewalls;

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

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

1.8.7 user access controls, and;

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

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.

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.

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.

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".

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

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

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

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.

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.

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

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.

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.

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.

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.

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.

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.

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:

1.24.1 Compliance with HMG Minimum Cyber Security Standard.

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.

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.

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.

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.

SCHEDULE 10

Exit Management

1. DEFINITIONS

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

Exit Information	has the meaning given to it in Paragraph 3.1 of Part A of this Schedule;
Exit Manager	the person appointed by each Party to manage their respective obligations under Part A of this Schedule;
Replacement Goods	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
Replacement Services	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
Termination Assistance	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
Termination Assistance Notice	has the meaning given to it in Paragraph 5.1 of Part A of this Schedule;
Termination Assistance Period	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of Part A of this Schedule;
Transferable Contracts	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
Transferring Contracts	has the meaning given to it in Paragraph 8.2 of Part A of this Schedule.

2. SUPPLIER MUST ALWAYS BE PREPARED FOR CONTRACT EXIT

2.1 Each Party shall appoint an Exit Manager within fourteen (14) Days of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

3. ASSISTING RE-COMPETITION FOR DELIVERABLES

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. EXIT PLAN

4.1 The Supplier shall, within fourteen (14) Days after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within ten (10) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) every thirty (30) Days throughout the Contract Period; and

(b) no later than five (5) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than five (5) Working Days after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than five (5) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. TERMINATION ASSISTANCE

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least thirty (30) Days prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than five (5) Working Days) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than three (3) Months after the date that the Supplier ceases to provide the Deliverables.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than three (3) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than ten (10) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than ten (10) Working Days' written notice upon the Supplier.

5.3 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. TERMINATION ASSISTANCE PERIOD

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. OBLIGATIONS WHEN THE CONTRACT IS TERMINATED

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. ASSETS, SUB-CONTRACTS AND SOFTWARE

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**), in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.4 The Buyer shall:

8.4.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.4.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.5 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.6 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to paragraph 8.3 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this paragraph 8.6 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. NO CHARGES

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. DIVIDING THE BILLS

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Contracts shall be apportioned between the Buyer and/or the Replacement Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

SCHEDULE 13

Implementation Plan and Testing

Part 1

Implementation Plan

1. AGREEING THE IMPLEMENTATION PLAN

1.1 The Supplier will provide a fully developed draft Implementation Plan for Approval within three (3) Working Days of the Start Date. The draft Implementation Plan shall be consistent with and reflect the invoicing timetable contained in Schedule 5 (Pricing Details)

1.2 The draft must contain enough detail for effective management of Contract implementation.

1.3 The Buyer shall not unreasonably withhold Approval of the updated draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it.

2. FOLLOWING THE IMPLEMENTATION PLAN

2.1 The Supplier shall perform its obligations in respect of Delivery and, where relevant, Testing of the Deliverables in accordance with the Approved Implementation Plan.

3. DELAYS

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

3.1.1 Notify the Buyer in writing within 2 (two) Working Days of becoming aware, explaining the likely impact of the Delay

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

Part 2

Testing

REDACTED

ANNEX 1

Test Plan

REDACTED

ANNEX 2

Testing Integration

REDACTED

SCHEDULE 14

Service Levels

REDACTED

ANNEX 1

REDACTED

ANNEX 2

REDACTED

SCHEDULE 15

Call-Off Contract Management

1. DEFINITIONS

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

Operational Board	the board established in accordance with paragraph 4 of this Schedule;
Project Manager	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. PROJECT MANAGEMENT

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day. The Supplier must also ensure Subcontractor (REDACTED) appoints a Project Manager for the purpose of this Contract.

2.2 The Parties, including Subcontractor (REDACTED), shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. ROLE OF THE SUPPLIER CONTRACT MANAGER

3.1 The Supplier's Contract Manager's shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. ROLE OF THE OPERATIONAL BOARD

4.1 The Supplier, the Subcontractor (REDACTED) and the Buyer shall be represented on the Operational Board to be established by the Buyer for the purposes of this Contract.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. CONTRACT RISK MANAGEMENT

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Contract which the Buyers and the Supplier have identified.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Operational Board

- Frequency of the Operational Board to be agreed within ten (10) working days of the Start Date.
- In compliance with Government's COVID-19 distancing rules, Operational Boards shall take place via a Virtual Meeting Platform. The preferred Virtual Meeting Platform will be the one proposed by the Buyer.
- Operational Board must have representatives from the Buyer, the Supplier and Subcontractor (REDACTED). It is the responsibility of the Supplier to ensure that (REDACTED) receive invites and have correct representation at the Operational Boards.

SCHEDULE 20

Specification

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyer under this Contract.

Buyer Requirements

The Buyer has engaged a programme through a separate procurement for disadvantaged children across England to receive laptops and tablets as part of an initiative to make remote education accessible for pupils staying at home during the coronavirus outbreak.

Devices will be ordered for children in the most vital stages of their education, those who receive support from a social worker and care leavers.

The Buyer also wish disadvantaged secondary school pupils and care leavers to have access to the internet – where those families do not already have mobile or broadband internet in the household. This requirement forms the scope of this Contract.

DfE Connectivity Device Catalogue

1. All devices shall be delivered direct to the Schools or Social Care Body delivery locations as ordered by the Responsible Body and will need to be configured to be usable 'out of the box' – they shall include all configuration necessary for pupils to operate them at home safely and securely for educational purposes.

2. The solution provided shall consist of the system set out in Annex A below.

3. Mifi Device delivery will be subject to a five (5) Working Day SLA from date of order and stock availability. Orders will be released on a first in, first out basis. The Long Stop Date for delivery of all the Roaming Sims and Mifi Devices is agreed as 30 June 2020.

4. The In-Life service will be supported by a reporting and helpdesk function as set out in Annex B below for use exclusively by the Buyer and Responsible Bodies.

5. Delivery of all MiFi Devices shall be co-ordinated with roll-out of Devices via the Supplier. To assist in communication relating to MiFi Devices, the Supplier can publish information (typically technical buying guidance, not personal information or serial number data) on the MiFi Devices on the ordering portal. This will be available to the Responsible Body's ordering users, not to schools or end users. Documentation must be agreed by the Buyer, and content approved by the Buyer, and sent to the Supplier from the Buyer before it is presented on the ordering portal.

6. The list of educational websites, including any exempt sites are set in in Annex C below.

ANNEX A

1. **Device Requirements**

1.1 MiFi Device to allow Internet access

1.2 Must include charging cable

1.3 MiFi Device must be configured with custom DNS settings

1.4 Must co-exist with the security service being used on portable devices, i.e. must not create any DNS issues/clashes

1.5 MiFi Device pre-configured to be usable 'out of the box' and locked down with a single admin ID/Password– this password will be restricted to an absolute need to know cadre of people involved in the delivery process, and must never be given to a Responsible Body or Local Authority or onwards to end users. The Supplier shall retain a record of users with access to the password. The Supplier shall make this available upon request from the Buyer.

1.6 Applied with a label containing generic wording to be pre-prescribed by the Buyer. The serial number of the actual device will be available to the end-user on the outside of the box in which it is delivered. The serial number of the SIM will be printed on the SIM, and the device and SIM serial numbers will be associated in an excel file.

1.7 Quick start guide in the box, to assist Responsible Bodies and children to set up the MiFi Device.

1.8 MiFi Device will only work with the Roaming SIM Card installed under this Contract; it will not work with any other third party SIM (dependent on maintaining security of the device admin password).

1.9 MiFi Device will come with a Warranty as set out in Schedule 5 Section 4.

2. **4G SIM Requirements**

2.1 4G/LTE SIM installed into Mifi Device or e-SIM configured

2.2 Data only Roaming SIM Card, no voice or text allowance

2.3 Minimum 3GB monthly allowance per Roaming SIM Card/MiFi Device

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

2.5 Pre-agreed means of adding additional data

2.6 Supporting removal of agreed whitelisted sites from data caps/allowances, as described in Annex C below.

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

2.8 Roaming SIM Card locked to MiFi device; Roaming SIM Card will not function with any other device unless requested by the Buyer

2.9 6-month contract, pre-purchased by the Buyer; option to extend on same terms at end of the Initial Period. Responsible Bodies given easy means to extend contract locally on same terms.

3. **Filtering Requirement**

3.1 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.

3.2 The Supplier shall procure that (REDACTED) and its associated 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.

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

3.4 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.

3.5 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.

3.6 Measures in place to prevent access to illegal internet content, specifically:

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

3.6.2 Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of The Home Office.

3.7 Inappropriate Online Content

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

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

3.7.2 Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances

3.7.3 Extremism: promotes terrorism and terrorist ideologies, violence or intolerance

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

3.7.5 Pornography: displays sexual acts or explicit images

3.7.6 Piracy and copyright theft: includes illegal provision of copyrighted material

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

3.7.8 Violence: Displays or promotes the use of physical force intended to hurt or kill.

3.8 This list should not be considered exhaustive and the Supplier shall produce reporting as per Schedule 1 (Transparency Reports) on this content.

ANNEX B

REDACTED

ANNEX C

Educational Sites (Inc exemptions)

The educational resources that telecommunications providers (Vodafone, EE, O2 and 3) have agreed with the Secretary of State for Education should be exempt from data charges. These resources will be included within the data allowances of this contract, until these exemptions are actioned by the telecommunications providers. The Buyer will update the Supplier as progress is made with the telecommunications providers.

Buyer Dependencies

REDACTED