Crown Commercial Service

RM 1557vii

G-CLOUD 7

Call-Off Agreement and Call-Off Terms

Schedule 2: Call-Off Terms

Effective Date	19/05/2017	**Order Reference**	STA-0158

FROM:

Customer	The Secretary of State for Education
Customer's Address	Sanctuary Buildings, Great Smith Street, London, SW1 3BT
Invoice Address	Standards and Testing Agency, SSCL Accounts Payable Team, Room 6124 Tomlinson House, Norcross, Blackpool, FY5 3TA
Principal Contact	Name:

TO:

Supplier	The Stationery Office Limited
Supplier's Address	29 St. John's Lane, London, EC1M 4NA
Account Manager	

1. TERM

1.1 Commencement Date

This Call-Off Agreement commences on: 19th May 2017

1.2 Expiry Date

This Call-Off Agreement shall expire on:

1.2.1 19th May 2019; or

1.2.2 the second (2) anniversary of the Commencement Date; whichever is the earlier, unless terminated earlier pursuant to Clause CO-9 of the Call-Off Agreement.

1.3 Services Requirements

1.3.1 This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilized by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

1.3.2 G-Cloud Services

1.3.2.4 Lot 4 **6153106362466304** - **Secure Application Development**

Specialist G-Cloud
Services

2. PRINCIPAL LOCATIONS

2.1 Principal locations where the services are being performed

Unless otherwise advised by the Customer, contract/service and performance meetings shall be held at one of the Customer's premises:

Coventry – Earlsdon Park

London – Sanctuary Buildings

2.2 Choice of venue shall be determined by the Customer and may take into account the Customer's intention to keep cost of travel and subsistence for all parties to a practical minimum and any engagement with other third party suppliers for the provision of the NCA tools Website.

3. STANDARDS

3.1 Quality Standards – Please refer to S3-32

3.2 Technical Standards – Please refer to S3-32

4. ONBOARDING

4.1 On-boarding

Please refer to Annex 1A - Mobilisation

5. CUSTOMER RESPONSIBILITIES

5.1 Customer's Responsibilities

As detailed in the Annexes

5.2 Customer's equipment

Not used

6. PAYMENT

6.1 Payment profile and method of payment

Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS

Please refer to S3-27

Indicate preferred payment profile by selecting one from:

6.1.1 Please refer to S3-27

6.2 Invoice format

Please refer to S3-29

7. DISPUTE RESOLUTION

7.1 Level of Representative to whom disputes should be escalated to:

First Level of Dispute

Customer – Ian Skidmore, Contract and Senior Materials and Systems Manager

Supplier –

Second Level of Dispute

Customer – Michael Pears, STA Test Operations, Head of Operational Delivery - Programme Management
Supplier –

Third Level of Dispute

Customer – Una Bennett, Deputy Director of STA Test Operations Division

Supplier –

7.2 Mediation Provider

Centre for Effective Dispute Resolution.

8. LIABILITY

Subject to the provisions of Clause CO 11 'Liability' of the Call–Off Agreement:

8.1 The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party under or in connection with this Call–Off Agreement shall in no event exceed £1 million.

8.2 The annual aggregate liability under this Call–Off Agreement of either Party for all defaults shall in no event exceed one hundred and twenty five per cent (125%) per cent of the Charges payable by the Customer to the Supplier.

9. INSURANCE

9.1 Minimum Insurance Period

One (1) Year following the expiration or earlier termination of this Call-Off Agreement

9.2 To comply with its obligations under this Call-Off Agreement and as a minimum, where requested by the Customer in writing the Supplier shall ensure that:

- **professional indemnity insurance** is held by the Supplier and by any agent, Sub-Contractor or consultant involved in the supply of the G-Cloud Services and that such professional indemnity insurance has a minimum limit of indemnity of one million pounds sterling (£1,000,000) for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time;

employers' liability insurance with a minimum limit of five million pounds sterling (£5,000,000) or such higher minimum limit as required by Law from time to time.

10. TERMINATION

10.1 Undisputed Sums Time Period

At least ninety (90) Working Days of the date of the written notice specified in Clause CO-9.4 of the Call-Off Agreement**.**

10.2 Termination Without Cause

At least three (3) months in accordance with Clause CO-9.2 of the Call-Off Agreement.

11. AUDIT AND ACCESS

Twelve (12) Months after the expiry of the Call-Off Agreement Period or following termination of this Call-Off Agreement.

12. PERFORMANCE OF THE SERVICES AND DELIVERABLES

12.2 The Implementation Plan as at the Commencement Date is set out below:

Milestone	Deliverables	Duration	Milestone Date	Customer Responsibilities
Exit Plan	Delivery of the agreed exit plan	3 months	31/08/2017	Agreement and input into proposed exit plan
Business continuity plan	Delivery of the agreed business continuity plan	3 months	31/08/2017	Agreement and input into proposed business continuity plan
Disaster recovery plan	Delivery of agreed disaster recovery plan	3 months	31/08/2017	Agreement and input into proposed disaster recovery plan
Service plan	Delivery of agreed service plan	3 months	31/08/2017	Agreement and input into proposed service plan
Project initiation document	Delivery of agreed project initiation document	1 month	30/06/2017	Agreement and input into proposed project initiation document
Security document	Delivery of agreed security document	3 months	31/08/2017	Agreement and input into proposed security document
Service guide	Delivery of agreed service guide	3 months	31/08/2017	Agreement and input into proposed service guide

12.2.1 If so required by the Customer, the Supplier shall produce within one (1) Month of the Commencement Date a further version of the Implementation Plan (based on the above plan) in such further detail as the Customer may reasonably require. The Supplier shall ensure that each version of the Implementation Plan is subject to Customer's written approval. The Supplier shall ensure that the Implementation Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation transition and/or transformation of the G-

Cloud Services.

12.2.2 The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

12.2.3 The Supplier shall perform its obligations so as to achieve each milestone by the milestone date.

12.2.4 Changes to the milestones shall only be made in accordance with the Variation procedure as set out in Clause CO-21 and provided that the Supplier shall not attempt to postpone any of the milestones using the Variation procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a milestone by the relevant milestone date).

12.3 Service Levels

Please refer Annex 1c of Service Requirements

13. [COLLABORATION AGREEMENT
1.1. The Customer does not require the Supplier to enter into a Collaboration Agreement.

BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES to enter a legally binding contract with the Customer to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read the Call-Off Terms and the Order Form and by signing below agree to be bound by the terms of this Call-Off Agreement.

For and on behalf of the Supplier:

Name and Title	
Position	
Signature	
Date	

For and on behalf of the Customer:

Name and Title	
Position	
Signature	
Date	

ANNEX 1 – SERVICE REQUIREMENTS

1. Background

1.1 Context

The Department for Education ("DfE" or "the Department") is responsible for the central administration of education and has the primary statutory duty of promoting the education of pupils in England and ensuring the effective implementation of education policy.

The Standards & Testing Agency “STA or “the STA” is responsible for National Curriculum Assessments and is an executive agency of the Department.

DfE has remitted Standards and Testing Agency staff to conduct this procurement on its behalf and STA will be the contracting authority for any contract awarded. From this point forward, where the term "STA" is used, it shall be taken to mean STA and / or DfE.

The STA has three main functions:

- To develop high quality and rigorous tests in line with Ministerial policy
- To undertake operational delivery of assessment (including printing, distribution, marking and data capture as appropriate)
- To support schools and other stakeholders to deliver the assessments.

The administration of the National Curriculum Assessments is via a website known as “NCA tools” and is accessed via https://ncatools.education.gov.uk/. NCA tools is a web based system that allows schools and local authorities, at Key Stages 1, 2 and 3 to administer National Curriculum Assessments and supply Teacher Assessment data. The Application is fully developed and the requirement is for a hosting, maintenance and development service for the Application.

From this point forward, where the term "Application" is used, it shall be taken to mean the NCA tools website.

The Application has been in existence since September 2008 and has been continuously developed and added to over the last 8 years. It provides a Management Layer which enables STA to manage users and schools, and a number of Modules for schools to carry out distinct activities throughout the school year. These Modules are Test Orders, Access arrangements, Teacher Assessment, Return of Results, Test materials and Headteachers declarations form. The Application enables schools to carry out Pupil Registration and view Test Scripts[1] by providing a single sign on into those external independent systems. The Application allows administrators from STA to view and maintain all parts of the Application including the underlying school and local authority data which is utilised throughout all modules. For the avoidance of any doubt, this does not include the ability to access Source Code, however the IPR in the system rests with the Department and the source code is lodged in Escrow. The Application also has a number of interfaces which enable STA to upload various sets of data, which are then automatically processed, from basic school information to pupil result data. Each of these Modules links with other systems and interfaces are described below:

<u>The Management Layer</u>

The core part of NCA tools is the Management Layer which enables STA to manage the whole application. The layer allows STA administrators to create, amend, delete and set access permissions for different users. It allows passwords to be reset or amended as well as the ability to suspend and release access to individual users. It also allows STA to upload school details, including address details, key stage information, amend those details and create and delete schools.

<u>Test Orders</u>

Test orders is a module which enables schools to place orders for Key Stage 1 and Key Stage 2. It also allows schools to place orders for modified versions, e.g. large print or braille, of the tests. The module is available throughout the year and access for schools is controlled by a calendar function. The module e-mails schools details of the orders that have been placed and allows administrators to download a number of reports giving details of the orders placed by schools.

[1] The hosting, maintenance and development of Pupil Registration and Test Scripts functionality is provided by a 3rd party, and does not form part of these requirements.

Access Arrangements

The Access Arrangements module allows schools to submit applications or notifications for a variety of reasons at either a pupil or whole cohort level, via a number of different forms and access for schools is controlled by a calendar function. These forms vary from allowing pupils additional time to take the tests, have an individual pupil or the whole cohort take the test at a different time or day to the scheduled time, allow the school to apply to open test papers early or notify STA if a pupil has been cheating in a particular test. In total there are currently nine different forms. A number of the forms simply require the school to notify STA of their intentions but other forms such as timetable variations require STA to approve the application. The module provides e-mail updates to schools with the progress of their applications. The module contains a secure messaging system which enables schools to communicate with STA staff about the applications that they are making. The module also contains a number of reports that provide STA and local authorities to download information about the applications that are made.

Teacher Assessment

The Teacher Assessment module allows schools to upload the teacher assessment data they have for their pupils at key stage 2. Schools can upload data in either a Common Transfer File (CTF), which is a XML file typically generated from the schools management information system (MIS), or via an Excel spread-sheet available from the module, which is pre-populated with the expected pupils for that school and is pre-formatted so that the schools can enter the data easily. The module allows schools and STA administrators to view the teacher assessment that has been loaded and amend and delete if necessary some of the data. The module also produces reports, which are downloadable by schools, LAs and STA administrators and formatted data feeds, which are sent to a third party to be matched to pupil results data.

Return of Results

Return of Results allows schools and local authorities to view and download the results of the national curriculum assessments that are sat in May and access for schools is controlled by a calendar function. . STA administrators upload pupil results data, which is automatically processed by the module, and displayed on different pages within the module according to subject. The upload for 2016 contains approximately 2.5 million lines of data and it is expected that this upload should take no longer than 1 hour to complete. A new piece of functionality was added in 2015 to enable key stage 3 schools to download item level data (answers to individual questions in the tests) for their incoming cohort. This upload for 2016 contained 4 million lines of data.

Test materials

The test materials module allows schools to download PDF versions of live materials controlled by a calendar. The module also allows schools to download Phonics test materials to assist in administering the Phonics screening check.

Headteachers declaration forms

The Headteachers declaration module allows schools to submit KS1, KS2 and Phonics headteacher declaration forms.

Links with other systems

NCA tools links via a secure single sign on mechanism, to a number of third party hosted applications, which are currently Pupil Registration, Script Return and Reviews. These third party systems allow pupils to register for the tests,view test scripts that have been marked via an onscreen marking application and apply for reviews. It is important to note that none of these systems share any data with NCA tools.

Interfaces/Automated processes

NCA tools contains a number of interfaces/automated processes that allow STA to update and amend data within the site. The following non-exhaustive list, details the main interfaces that are in place.

- Edubase update – this allows STA to load details of all schools into the application and contains various fields which defines the school information present in NCA tools.

- Remove list – this allows STA to remove closed schools from the application and also contains information on how existing data should be migrated between schools.
- Teacher assessment pupil list – this allows STA to upload a list of pupils into the teacher assessment module, which can then be downloaded by schools and LAs.
- Pupil results – an automated process, which takes a file of pupil results data and pupil results item level data and uploads it into the Return of Results module.

Most of the above processes are automated and are triggered by STA uploading a file into a specific location within a SFTP site provided by the supplier of NCA tools.

The targeted date for completion of contract award is 18 April 2017, with transition of the system to be completed for commencement of live service on 19 May 2017.

If deemed necessary a third party company (NCC Group) will undertake a Build Assured Verification exercise to provide assurance to potential bidders that a fully working system can be built from the code placed into Escrow if required. The report will be made available prior to contract award.

1.2 Design and Brand

The look and feel of the Application (https://ncatools.education.gov.uk/) mirrors that of www.gov.uk and notice should be taken for future development of the colour palettes used, page structure/design and renditions (see 2.3.3).

1.3 Scope of Services

The outline requirements for the Application include:

- Managed hosting service;
- Support service - to include rectification of defects and full incident and problem management to resolution; Limited to 45 calls per year not including calls resulting from defects caused by TSO action;
- Maintenance - to include minor site enhancements such as changes to form fields and changes to static text (between cycles i.e. from 2016 >> 2017); and
- Development - to include system changes resulting from policy change, continuous improvement and/or to improve system functionality and the testing of those changes.

The modules listed above currently support Key Stages 1, 2 & 3. During the term of the contract, this scope may extend to other Key Stages and any such extension(s) is in-scope of this procurement.

The Supplier is requested to review the requirements specification described in section 2 and propose a plan and fixed cost for implementing in line with the timescales noted in section 1.1 of this document. They should detail key personnel, key dates and technical features within the plan. Assumptions, risks and dependencies are also to be clearly stated.

2. Requirements

Statement of Requirements	
2.1 General	
2.1.1	The Supplier must hold, and permit STA open access to, detail relating to all activities undertaken in delivering the Services.
2.1.2	The Supplier must cooperate with STA in all requests for assistance in satisfying any requests for information from Ofqual or any other regulatory body, this for example could include Freedom of Information requests.
2.1.3	The Supplier must attend any meetings as reasonably requested by STA at locations determined by STA – including Earlsdon Park, Coventry and Sanctuary Buildings, London.

2.1.4	The Supplier must facilitate a productive working relationship with STA and other key stakeholders, including: • Effectively communicating and sharing information in a manner that supports the smooth running of the Service; • The provision of evidence-based assurance to STA that the Service is being delivered accurately, on time and securely; • Showing flexibility in responding to changes in Assessment policy as determined by Government priorities; • Driving Service improvements and efficiency savings; • Recognising that protecting and enhancing the Government's reputation matters as much as that of the supplier.
2.1.5	The Pupil Level Data collected by the Application during the life of the contract is classified as Official - Sensitive. The Supplier should ensure and provide assurance to STA that all systems and processes handling this data are secure and congruent with this level of data classification.
2.1.6	The Supplier must provide any information required by STA to comply with any regulatory or legislative obligations.

2.1.7	The Supplier will ensure the Application is supported by an infrastructure capable of ensuring a good service for the following estimated usage metrics: General (NCA tools Portal) • NCA tools Portal is used throughout the whole year • Total number of schools and local authorities circa 20,000 • Total potential number of users circa 100,000 • Maximum number of estimated concurrent users circa 1,000 • Maximum number of logins per day, circa 30,000 – 50,000 • Number of schools accessing "linked" websites, circa 30,000 – 50,000 • Storage requirements for each module - 147 Mb - Access Arrangements - 2gb - Pupil Results - 197 Mb - Teacher Assessments - 451 Mb - Test Orders • There are 172 downloadable test material files in the system that include Zip files, PDF file and word files. The total size is 366Mb. The average file size is 2Mb with the lowest file size being 15KB and largest file size being 77Mb. <u>Test orders:</u> <u>Please note: the figures below are based on historical usage and due to a change in assessments it is anticipated that the number of schools placing test orders will reduce dramatically over the life of this contract.</u> • Test orders is used between October – May • Number of schools placing KS1 test orders circa 2,000. Each test order can be for up to 3 products. • Number of schools placing KS2 test orders circa 2,000. Each test order can be up to 3 products. <u>Access arrangements</u> • Access arrangements is used between January – June • Number of access arrangements applications circa 30,000 <u>Key Stage 2 (KS2) Teacher Assessment</u> • KS2 Teacher assessment is collected from May - September. • KS2 Teacher assessment is collected for circa 600,000 pupils. <u>Return of Results</u> • Return of Results is used between July – January • Number of results returned for pupils circa 1.8 million (based on 600,000 pupils sitting 3 tests each). The size of the upload file for 2016 was 370mb and contained 2.5 million lines with each line containing approximately 38 fields of data. • The size of the item level file was approximately 600mb and contained 4 million lines of data with each line containing approximately 80 fields. <u>Headteacher's declaration forms</u> • Phonics screening check is used between May – July • Number of schools completing HDF form circa 16,500 <u>Test Materials</u> Number of schools downloading materials circa 17,000

2.1.8	Relevant standards and methodologies should be adhered to; these might include, but are not limited to • ISO9001: Quality Management System • ISO/IEC 27001: Information Management Security System • BS 25999 or ISO 23301: Business Continuity Standard • ISO/IEC 24762: IT Eer Recovery • HMG Security Policy Framework (SPF) • PRINCE2 (Projects in controlled Environments) • ITIL (Information Technology Infrastructure Library) • MoR (Management of Risk)
2.1.9	The Supplier will ensure that its solution for the delivery of the service meets the Department for Education's (DfE) information standards and is flexible enough to support new and updated standards as and when they are published. The Supplier will ensure that their systems follow the principles of data management – ensuring master copies are held and accessible in emergency. The Supplier shall ensure that any data that is presented for transfer, between the Supplier and STA, is in a format agreed by STA and must ensure that all data feeds are technically compliant with the Common Basic Data Set (CBDS).
2.1.10	The Supplier will ensure the Application delivers an average Transactional Response Time of no greater than 2 seconds to the perimeter of systems within the Supplier's network. The transaction will be measured from the time the Supplier receives the instruction to perform the transaction and is delivered to the perimeter of the systems within the Supplier's network. The average will be calculated over a monthly period. Transactional operations include the submission of applications and the retrieval and display of data.
2.1.11	The Supplier will ensure the Application delivers an average non-Transactional Response Time of no greater than 1 second to the perimeter of systems within the Supplier's network. The transaction will be measured from the time the Supplier receives the instruction to perform the transaction and is delivered to the perimeter of the systems within the Supplier's network. The average will be calculated over a monthly period. Non-transaction operations include the display of help text, menus and other navigational assets.

2.1.12	The Supplier will ensure that the Application is available 24 hours a day with an Availability of at least 99.8%. The Availability will be calculated on a monthly basis and will exclude any Routine Maintenance that can be carried out in a window between 12am and 4am daily, by prior arrangement with STA. For Application Availability, the percentage Availability shall be calculated over a calendar month using the following equation: (B-A)/B*100=AVAILABILITY% Where: A – Total amount of time (in minutes) that the Application was not available during the relevant calendar month B – Total amount of time (in minutes) in the relevant calendar month excluding the total amount of time (in minutes) that the Application was not available as a result of Scheduled Maintenance. e.g. if a month has 31 days and the website is not Available for 30 minutes, with 10 minutes of Scheduled Maintenance, then the percentage Availability shall be calculated as: A=30, B=(31*1440)-10=44630 (44630-30)/44630*100=99.93%
2.1.13	The Supplier will provide STA and/or its nominated representative(s) access to the Application as per requirement 2.3.7.
2.1.14	The Supplier will ensure that any remote access tools comply with the security requirements of STA.
2.1.15	The Supplier must ensure that the following documentation is available for its solution and describes the architecture and components in sufficient detail that any successor operator or users not involved in the initial development can use, install, operate and maintain the Application. This should include but not be limited to: 1. A design document with architectural diagrams describing the solution infrastructure; 2. Interface documentation containing details of interfaces to other elements of the Application and modules where information is shared; 3. A technical specification document defining the technical aspects of the Application, including the standards to which they have adhered (noting that the Cabinet Office guidelines insist that procured Application are based upon recognised open standards where they exist); 4. A functional specification document or equivalent defining the functional operation of the Application; and 5. Documentation of operation and user processes. The Supplier will put in place the necessary measures to keep this documentation up to date and available to STA on request and in accordance with the agreement.
2.1.16	The Supplier must transfer data securely between the supplier and STA, and between the supplier and any of its Subcontractors or other persons involved in the delivery of the Service as specified by STA.
2.1.17	STA may request the Supplier to provide development services during contract term. Further details relating to the provision of these development services (including full specifications and price) shall be agreed through the Change Control Procedure from time to time.

2.1.18	STA may request certain activities to be completed outside of those covered under development services in order to prepare the modules for live service; these activities are expected to be carried out as maintenance of the system. They include, but are not limited to: 1. Updating downloadable materials, including menu descriptions and the actual files to be downloaded. These materials are available within Test Materials, but if they are introduced within other modules then these should also be included. 2. Updating of text that is not covered by content management system (CMS) templates. This includes items such as rolling over dates and updating text so that it is suitable for the new academic cycle. 3. Minor changes to page design, including items such as headings within forms and updating of text contained within forms. 4. Clearing out of previous cycles' data in readiness for go-live of a particular module. 5. Ensuring users have to reset their passwords on at least an annual basis 6. Updating and maintaining licenses including those required to maintain the single sign on function between NCA tools and externally hosted sites.
2.1.19	The Supplier will ensure they put in place the necessary infrastructure to ensure the automated uploads of data by STA, referred to in the background section of this document, and are supported for all current functionality. In particular the solution should ensure that the results data is uploaded in its entirety inside a maximum of 4 hours.
2.2 Project Management, set-up and transition	
Project Management	
2.2.1	The Supplier must manage all aspects of set-up in accordance with PRINCE2, ITIL and Management of Risk (MoR) or similar methodologies agreed in advance with STA.
2.2.2	The Supplier must submit a Project Initiation Document (PID) to be agreed by STA which clearly sets out the project from the outset. This document shall be consistent with PRINCE2 (or similar) controls and cover all aspects of the Set-up of the project.
2.2.3	The Supplier must ensure that any development to the solution is carried out and documented to industry accepted standards, as agreed with STA. The Supplier must make available, upon request, any System documentation for inspection by STA, including documentation on the progress of development.
2.2.4	The solution will be subject to Operational Acceptance Testing to ensure it is ready to go live following set-up and any subsequent change to any Module. Whilst the decision of Acceptance rests with the STA, the Supplier must provide appropriate industry standard evidence, agreed in advance with STA, to STA that Operational Acceptance Testing has been carried out, addressing functionality, capacity, security, performance, availability and resilience. Acceptance will include testing of processes and procedures as well as of the Systems. The Supplier must produce a test strategy and plan, for the approval of STA. During each change during the contract term, the Supplier must ensure that the agreed test strategy and plan are adhered to for all aspects of their solution employed in delivering the Service. The test strategy and plan will be reviewed for each Test Cycle during the contract term. Where a change is to be made to the solution, the Supplier must agree, with STA, the scope of the testing for the changes and the associated Acceptance Criteria prior to any System development or testing taking place. The Supplier must define and agree a set of documentation that will be provided to STA alongside each deliverable throughout the life of the contract.

2.2.5	Software owned by STA or developed by the Supplier in provision of the Services must comply with open standards and must be portable at the effective date of the expiry or termination of the Agreement.
2.2.6	The Supplier must ensure that the following documentation is available for its solution (following set-up and after any change to any of the applications) and describes the architecture and components in sufficient detail that any successor operator or users not involved in the initial development can use, install, operate and maintain the solution. This should include but not be limited to: 1. A design document with architectural diagrams describing the solution infrastructure; 2. Interface documentation containing details of interfaces to other elements of the Solution and modules where information is shared; 3. A technical specification document defining the technical aspects of the solution, including the standards to which they have adhered (noting that the Cabinet Office guidelines insist that procured solutions are based upon recognised open standards where they exist); 4. A functional specification document or equivalent defining the functional operation of the solution; and 5. Documentation of operation and user processes. The Supplier will put in place the necessary measures to keep this documentation up to date and available to STA on request and in accordance with the Agreement. The supplier should provide product descriptions for the above documents which are to be agreed in advance with STA.
Set-up	
2.2.7	The Supplier must provide a Project Plan detailing the resources, tasks and timescales required to be performed for Set-up and to Transition the Services into Live Service together with a summary milestone plan which details the deliverables outlined in the Project Initiation Document, and requirements / dependencies upon STA.
2.2.8	By the date for the completion of Set-up the Supplier must have: • All systems, business processes and infrastructure built, installed, fully tested and accepted by STA including an end to end test to demonstrate that the required data outputs are produced by the systems intended for use in the delivery of Services; • Completed and provided to STA all specifications and completed the building of all systems which will be used to support the delivery of Services; • Recruited all key persons; • A Security Document which has been agreed with STA. • A Business Continuity Plan and Disaster Recovery Plan, which has been agreed with STA; • Agreed an initial Exit Plan and initial Exit Information Document with STA; • Awarded contracts for any elements of the Service that will be delivered by Subcontractors; and • A Service Plan agreed with STA.
2.2.9	The Supplier must discuss and demonstrate to STA the readiness and appropriateness of plans, processes, systems, resourcing and any other factors required to enable the reliable completion of the work. Plans are to be kept up-to-date and communicated to STA weekly or as required.
Transition	

2.2.10	Prior to go-live of the Live Service, the Supplier shall produce and maintain a Service Guide to be used by the Supplier and STA's Service Management teams during service management. The guide shall be written in layman's terms and contain, as a minimum, the following sections: • Technical Overview • Incident Reporting and Management Procedures • Service Levels and Service Credits • Management Information and Reports • Change Management • Escalation Procedures and Key Contacts
2.3 Technical Requirements for the current applications	
2.3.1	The Supplier must ensure that the .NET platform and Source Code written in C# or HTML5 as appropriate is maintained.
2.3.2	The Supplier must ensure that the Application shall utilise an SQL 2012 R2 database. Additionally, the Supplier must be able to demonstrate the capability to upgrade from SQL 2012 R2 to a later version of SQL.
2.3.3	The Supplier will ensure that the Application conforms to the STA style and branding guidelines and information architecture.
2.3.4	The Supplier shall at all times maintain all documentation associated with the Application in line with accepted Industry Standards. The Supplier will provide copies of the documentation to STA at any time on request.
2.3.5	The Supplier must provide a duplicate of any external facing system (a test environment) for the use of STA during the Test Cycle. This duplication must extend to the versions of operating systems and databases present on the live system. Any Test Environment must be Available for a minimum of 95% during the hours of 7am to 7pm, Monday to Friday. There may be a requirement to utilise the Test Environment out of these hours and STA should be informed if there are any planned outages of the Test Environment.
2.3.6	The Supplier must retain all STA data and maintain its integrity until handover to STA at the end of the contract term or ensure its secure destruction, providing evidence to STA to confirm this action.
2.3.7	The Supplier must continue to ensure Access Control is enforced such that the appropriate user can access the appropriate function within the Application. This includes the addition and removal of users from the Application. NB. The list of users will not be limited to STA employees and may include representatives of STA, other STA service providers and other relevant stakeholders.
2.3.8	The Supplier will allow appropriate STA staff to have access to the raw data contained within the Application: access will be controlled to ensure that it does not compromise data integrity. The supplier will agree a method with STA as to how STA accesses this data.

2.3.9	The Supplier must ensure that any development to the Application is carried out and documented to Industry Accepted Standard, as agreed with STA. The Supplier must make available, upon request, any Application documentation for inspection by STA, including documentation on the progress of development. The Supplier must provide an Application development strategy for agreement with STA. In addition the Supplier must agree with STA the changes that are to be made to the solution before any development work is carried out.
2.3.10	The Supplier must ensure that the Application remains compatible with a set of common browsers, which meet a minimum of 95% total coverage of UK browser usage, and are supported by the manufacturer of those browsers. The Supplier must provide a list of browsers with which the Application is compatible and ensure that this list is updated and agreed with STA on at least an annual basis during contract term, taking into consideration developments of browsers throughout.
2.3.11	The Supplier must ensure that any future Development must support web accessibility and is (at a minimum) compliant with AA of the W3C Web Content Accessibility Standards, see references below. Additionally, within the first 6-months of operation, the Supplier must ensure any elements of the Application which is not compliant with AA of the W3C Web Content Accessibility Standards, shall be updated accordingly. The Supplier must seek independent accreditation of its solution and provide evidence in terms of a certificate or statement of compliance to STA. Where possible with new developments the Supplier should seek to make those developments AAA compliant, subject to time and materials. If 3rd party certification is required to prove the AA rating of the current application – these costs will be passed to STA. If any modules are found to not meet AA: TSO will fix at own cost. References: http://www.w3.org/TR/WCAG20/ http://coi.gov.uk/guidance.php?page=131
2.3.12	The development, testing and deployment of the Application must be controlled under best practice Configuration Management arrangements through the provision of tools and processes for configuration control aligning with ITIL v3 best practice, or equivalent. This includes: • Maintenance of a configuration library containing all items under configuration control • Maintaining version control for all configuration items • Testing and release management processes
2.3.13	The Supplier must ensure that the Application enables all electronic transactions committed through the user interface to be audited including information such as but not limited to: 1. User 2. Time 3. Date 4. IP Address 5. Log-ins 6. Details of change The Supplier must make such audit data available on request to STA and make such data available in a person-readable format.

2.3.14	The Application must undergo a rigorous testing before its introduction into Live Service. The Supplier will produce a testing strategy and associated plan for the delivery of the Application, which will be subject to review and sign off by STA. The following requirements should form a minimum basis of any test strategy and plan: • Testing shall cover the functional and non-functional requirements; • STA User Acceptance Testing (UAT). The supplier will be obliged to consider feedback from these UAT activities and implement changes as necessary; • If for any reason a change is made to the Application post-assurance then the Supplier must provide evidence of a full regression test as well as targeted testing for the change; • The Supplier will ensure that the Application will be penetration tested by a CESG accredited company by a date to be agreed with STA. The scope of the penetration test should be shared with STA before the test takes place. The penetration test report is to be provided to STA along with any proposed remedial action for issues contained within the report; and • The Supplier will load test the Application using either an independent third party or internally using an Industry Accepted Standard load testing tool. The Supplier will ensure that the strategy and parameters for the load testing are agreed in advance with STA before any load testing is carried out and provide the results of the load testing to STA.
2.3.15	The Supplier must provide appropriate Industry Accepted Standard evidence of their internal testing, addressing functionality, capacity, security, performance, availability and resilience, including but not limited to: • Test scripts • Defect report • System sign-off documents • Deployment report • Load test report • Penetration test report
2.4 Hosting Requirements	
2.4.1	The Supplier must ensure that the Application is capable of being hosted securely within an Official – Sensitive environment. All STA data held by the Supplier for the duration of the contract will be kept logically separate from the data of any of the Supplier's other service recipients.
2.4.2	The Supplier must provide sufficient bandwidth for the Application to ensure that the Application functions efficiently. The Application shall show no degradation of services where usage is equal to or below 120% of the maximum estimated concurrent users (circa 1,000). The Supplier must be able to produce performance testing data verifying bandwidth usage.
2.4.3	The supplier will provide secure hosting facilities with appropriate physical, technical and procedural controls embedded. Guidance on the required controls should be sought from the HMG Security Policy Framework located on GOV.UK https://www.gov.uk/government/publications/security-policy-framework
2.4.4	The Supplier will ensure that all Routine Maintenance is carried out during a daily window of 12am to 4am. The Supplier will notify STA of any Scheduled Maintenance required to be undertaken outside this window and the reason for the maintenance at least 10 working days in advance of the maintenance being performed.

2.4.5	The Supplier will notify STA retrospectively of any Emergency Maintenance that has been undertaken and the reason for the Emergency Maintenance, where this has not been carried out with the prior agreement of STA. Any Emergency Maintenance performed outside of the daily maintenance window will count as downtime for the calculation of Availability. Emergency Maintenance will include the application of any critical security patches that are required to protect the Application / Service offering.
2.4.6	The Supplier will host the Application on a domain or sub-domain as specified by STA and will support any transition to a single government domain that may be required in the future.
2.4.7	The Application shall be capable of connecting to external applications (for example Pupil Registration) and shall not require users to provide additional login credentials over and above the single sign on solution which is currently NCA tools (https://ncatools.education.gov.uk).
2.4.8	The Supplier will carry out any necessary Routine Maintenance where it reasonably suspects that the Application has or may have developed a fault. Without prejudice to any other provision of this document, any such Routine Maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the normal operation of the Application. Critical security patches may need to be applied as Emergency Maintenance. The Supplier shall notify STA prior to carrying out any Emergency Maintenance work, unless the Supplier reasonably believes that providing such notification would delay the carrying out of any critical Emergency Maintenance work.
2.4.9	The Supplier shall issue a Release Note for each update and upgrade it releases in respect of the Application. The Supplier shall ensure that such Release Notes: (a) are user-friendly and are capable of being used and understood by reasonably skilled technical staff responsible for installing the update or upgrade; and (b) describe any changes to the front-end of the Application, as such front-end would appear to users.
2.4.10	The Supplier shall put an effective and appropriate Configuration Management procedure in place in accordance with Industry Accepted Standard, to establish and ensure the consistency of the Application's performance and its functional and physical attributes and conformance with the Application requirements and operational characteristics during the contract term.
2.4.11	The supplier will advise STA of any proposed changes to agreed hosting arrangements, including the adoption of cloud hosting of the services delivered to the STA.

2.5 Service Management	
2.5.1	The STA's approach to Service Management is aligned with ITIL version 3, see reference below. The Supplier must ensure that its approach to Service Management is aligned with ITIL version 3. The reference for all ITIL related references in this section can be found at: http://www.itil-officialsite.com

2.5.2	The Application must undergo rigorous testing following any system development work or significant change to the supporting infrastructure. The Supplier will produce a testing strategy and associated plan for the delivery of the Application, which will be subject to review and sign off by STA. The following requirements should form a minimum basis of any test strategy and plan: • Testing shall cover the functional and non-functional requirements; • STA User Acceptance Testing (UAT). The Supplier will be obliged to consider feedback from these UAT activities and implement changes as necessary; • If for any reason a change is made to a system post-assurance then the Supplier must provide evidence of a full regression test as well as targeted testing for the change; • The Supplier will ensure that the Application will be penetration tested by a CESG accredited company by a date to be agreed with STA. The scope of the penetration test should be shared with STA in advance of the test taking place. The penetration test report is to be provided to STA along with any proposed remedial action for issues contained within the report; • The Supplier will load test the Application using either an independent third party or internally using an industry standard load testing tool. The Supplier will ensure that the strategy and parameters for the load testing are agreed in advance with STA before any load testing is carried out and provide the results of the load testing to STA.

2.5.3

The Supplier must document its approach to Incident and Problem management, which must align with ITIL version 3. The Supplier will be responsible for the resolution of all Incidents and Problems that are raised by STA.

The Supplier must categorise each Incident and Problem and provide STA with the category and proposed time for resolution.

The Supplier will use the severity scale to categorise any incident or request that is raised by STA. This scale is as follows:

Priority Level	Response time	Description
P1	The Supplier shall resolve the issue using reasonable endeavours, where possible within 2 business hours, working continuously until the fault is resolved. In addition, the Supplier shall inform STA within one hour of being aware of the issue and shall provide update every 2 business hours until resolution.	Application unavailable or issue impacting over 25 Users meeting their submission deadlines for applications and notifications that the users make on the Application.
P2	The Supplier shall resolve the issue using reasonable endeavours, where possible within 4 hours. In addition, the Supplier shall inform STA within 2 hours of being aware of the issue and shall provide an update every 4 hours until resolution.	Application response time exceeds the Transactional Response or over 25 Users have reported intermittent Faults
P3	The Supplier shall resolve the issue using reasonable endeavours, where possible within 2 business days. In addition, the Supplier shall inform STA within one business day of being aware of the issue and shall provide an update every 2 business days until resolution.	More than 10 but fewer than 25 users have reported intermittent faults
P4	The Supplier shall resolve the issue using reasonable endeavours, where possible within 5 business days. In addition, the Supplier shall inform STA within 2 business days of being aware of the issue and shall provide an update every 2 business days until resolution.	Business impact is not critical; likely to include Application changes which can be made without affecting user Service.
P5	STA informed of estimate	Low business impact such as a request for work in the future.

2.5.4

The Supplier must document its approach to Availability Management which aligns with ITIL version 3.

The Supplier will ensure that the Application is Available for a minimum of 99.8% of the time.

Availability will not include periods of planned Routine Maintenance, which must be agreed in advance with STA.

Any Test Environment must be Available for a minimum of 95% during the hours of 7am to 7pm, Monday to Friday. There may be a requirement to utilise the Test Environment out of these hours and STA should be informed if there are any planned outages of the Test Environment.

2.5.5	The Supplier must define its approach to Capacity Management which must align with ITIL version 3. The Supplier must develop a Capacity Plan to demonstrate how the Supplier will manage identified patterns of business activity and the potential for growth of users and data over the contract term if for example key stage 4 schools were given access to the system following a policy decision.
2.5.6	The Supplier must define its approach to Service reporting which must align with ITIL version 3. The Supplier must provide Service Management reports to STA in advance and in-line with its existing Service Management requirements which currently utilise a monthly service report cycle. Additionally the Service reports must be made available to STA on request. The Service reports must include, but not be limited to, a management summary and detailed breakdown including: • Availability / non availability; • Incidents and problems raised, resolved and outstanding; • Impact assessments; • Minor enhancements; • Risks and issues; • Performance against Service Levels; • Forward plans; • Service metrics; and • Service call response times and any target breaches.
2.5.7	The Supplier must define its approach to Change and Release Management which must align with ITIL version 3. The Supplier must ensure that any change to the Application is authorised by STA. The Supplier must document (and agree with STA) its Change and Release management process. The Supplier's Change and Release management process documentation should include (at a minimum): • Details of change windows; • Details of pre-planned outages; and • Release schedules.
2.5.8	The Supplier will ensure that the Technical Support Desk[2] is available during the following times: 08.30 to 17.30 during weekdays, excluding Bank holidays.
2.5.9	During July, the Supplier will provide an out of hours technical support service to ensure the delivery of Return of Results.
2.5.10	If the Supplier fails to provide the Services in accordance with the Service Levels then Service Credits shall become payable by the Supplier.
2.6 Resources	
2.6.1	The Supplier must have suitably qualified and experienced staff (or immediate plans to access these resources as appropriate). Skills and qualifications of identified key personnel should cover all major aspects of the Service including commercial management, project management, technical skills and general management.
2.6.2	The Supplier must agree with STA which posts are considered as key posts, where knowledge or skills are critical to success.
2.6.3	The Supplier must provide advance notification to STA of any changes in key personnel; replacements should have equivalent skills and qualifications.

[2] For clarity, this is a STA helpdesk for incident logging by Systems team, not an external end user (school/LA) facing helpdesk.

2.6.5	The Supplier must ensure any resource related risks are documented within the Risk Log.
2.7 Subcontractors	
2.7.1	The Supplier must demonstrate that, where there are plans to use a Subcontractor, the Subcontractor is reliable, available and can meet the obligations imposed on the Supplier under this agreement. The Supplier must provide and maintain details of who these resources are, how they will be used and how they will be managed. The Supplier will provide STA with its procurement strategy and selection criteria for all Services which they intend to Subcontract. The Supplier will advise STA of the progress of its procurement activities against the agreed plan and inform STA of the nominated preferred bidder prior to contract award.
2.7.2	The Supplier must require that any subcontractor(s) are operating acceptable security policies, in line with the HMG Security Policy Framework and must confirm that this is the case prior to letting the relevant subcontract(s). The Supplier must provide STA with copies of a completed Security Policy Framework matrix for each Subcontractor. The Subcontractor must agree to security audits by STA where required.
2.8 Quality	
2.8.1	The Supplier must adopt quality standards that adhere to ISO9001: Quality Management System.
2.8.2	The Supplier must ensure that all project staff engaged in the delivery of the Services have a level of knowledge of the contractual terms and conditions commensurate with the level of their responsibility and involvement
2.9 Management Information and Reporting Flexible Management Information and reporting tools are required throughout the process to allow STA and other authorised parties to monitor progress and manage planned and unplanned interventions.	

2.9.1	Management Information shall be provided in MS Word (or similar) or MS Excel (or similar) format and shall cover a minimum of the following headings:

	Title of Management Information	Content
1	Incidents	Raised, Outstanding, Resolved, Response times
2	Changes	Raised, Outstanding, Resolved.
3	Support Requests	Raised, Outstanding, Resolved, Support availability
4	Service Level performance details	Availability, Support Desk Availability (required and achieved)
5	Application usage details	Number of users accessing the system, Number of Access arrangement Applications by application type (Approved, Pending, Rejected)
6	Security	Details of any potential security requirements and other security breaches
7	System Performance details	Average memory usage, Total disk space, Average processor usage, Database size (for database servers only), Number of database locks (for database servers only), Number of failed backups (for database servers only)
8	Service Levels and Service Credits	Performance of the Services against the Service Levels and details of Service Credits triggered
9	Web-based statistics	Trend information similar to Web-trends or Google Analytics that would show number of visits, average visits per day, duration, browser version breakdown, platform breakdown and similar.

2.9.2	In addition, the Supplier must: • Provide ad hoc information and/or reports as required by STA; • Provide Management Information within timescales and frequencies to be agreed with STA to monitor system performance, availability and demand on or take up of system functionality and reassure the STA of proper performance; • Provide access to STA of the source data from which Management Information is generated on request and without unreasonable delay.
2.10 Equalities	
2.10.1	The Supplier will at all times comply with and require that its Subcontractors comply with the Equality Act 2010.
2.11 Security	

2.11.1	The Supplier must provide contact details of the person who has ultimate responsibility for all aspects of information governance and security management relating to the Supplier and any Subcontractors delivery of the Service, including: • The specification and implementation of appropriate security policies and standards, specific to the Service being delivered, that comply with the current version of the HMG Security Policy Framework (SPF), ISO/IEC 27001 / 27002 or the Cyber Essentials Scheme;' • Monitoring compliance with the security policies; • Notifying STA of any security breaches; • Reviewing and updating the risk log with security related risks; • Monitoring the security performance of any appointed Subcontractor(s) and ensuring their Service delivery complies with the most recent HMG SPF; • Providing STA with regular Management Information reports; • Reviewing and updating the security risk log; • Security performance of any Subcontractor(s) complies with the HMG Security Policy Framework (SPF); • Ensuring compliance with CESG Good Practice Guides (GPG) in the delivery of the Service, where appropriate; and The security plan shall be reviewed and approved by STA and, if necessary, updated to meet STA requirements prior to the commencement of the Services.
2.11.2	The Supplier shall follow the requirements of the Government Security Classification Policies located on GOV.UK and will work with the STA to identify any materials or data which require classification. This shall include all information to which the Supplier and any Subcontractors may have access, such as; Pupil Level Data or Secure Test Materials. The Supplier shall register and maintain a log of all such materials, which shall be available to STA, on request.
2.11.3	The Supplier must make all personnel aware of the Supplier's security policies and standards (including the HMG SPF) during their induction, or at the commencement of their employment by the Supplier. Supplier personnel must then sign a declaration that they have understood and will comply with the security policies. The Supplier must ensure that these declarations are retained, and can be inspected by STA on demand.
2.11.4	The Supplier must undertake a business-driven risk assessment process, in line with the Cabinet Office Security Policy, to cover all aspects of using an Industry Accepted Standard structured methodology such as ITIL, ISO 27001, Cabinet Office Security Policy Framework or ISO 23301 to determine the likelihood and impact of potential vulnerabilities, threats and adverse events. The Supplier must actively manage all identified security risks and regularly review and update the associated risk log.
2.11.5	The Supplier must provide a security document, for approval by STA. The security document must be based on, and compliant with, the principles of ISO/IEC 27001, incorporating detailed security policies, standards and controls. This security document shall cover all aspects of the Supplier service, and that of all Subcontractors, including physical security, infrastructure, platforms, applications, services and interfaces. The Supplier must adhere to the agreed security document and complete the activities detailed in the plan, recording evidence of the completion of activities as part of a monthly security report for STA.

2.11.6	The Supplier must specify and implement a security policy and standards, specific to the Services that are delivered. The policy and standards will be based on and comply with the principles of ISO/IEC 27001 and applicable Government policies. The policy shall include: • Securing, controlling and monitoring access to buildings and data; • Control and encryption of sensitive electronic data in transit across the internet or network, data at rest on servers and other devices, including memory sticks; • Ensuring no sensitive material is left on desks for any period of time; • Suitable and secure storage of all hard copy sensitive material; • Ensuring appropriate responsibilities and duties of all staff with regard to security; • Communication of such responsibilities and duties to staff; • Security checks on personnel, subcontractors and temporary personnel with access to sensitive information and materials, including baseline personal security standard (BPSS) checking of people with access to Pupil Level Data; • Control of the transfer of sensitive material outside the organisation, with appropriate authorisation and signature; • Regular review and testing of this policy; and • Records of security audits and breaches of security. The Supplier's security policy must be provided to STA for approval.
2.11.7	The Supplier must require that any Subcontractor(s) are operating acceptable security policies, in line with the HMG SPF and must confirm that this is the case prior to letting the relevant Subcontract(s). The Supplier must provide STA with copies of a completed Security Policy Framework matrix for each Subcontractor. The Subcontractor must agree to security audits by STA where required.
2.11.8	The Supplier must provide STA with the right to access to locations from which the Services are being provided or managed so that STA may verify any suspected security issues.
2.11.9	The Supplier must provide STA with details of their secure file transfer solution e.g. Secure File Transfer Protocols (SFTP). All mechanisms for data transfer must be approved by STA before use in delivery of the Service.
2.11.10	The Supplier must ensure that no materials or data related to the Services shall be transferred or processed outside of the European Economic Area (EEA) at any time, unless STA has given its explicit consent to such transfer or processing.
2.11.11	The Supplier must ensure that adequate fire prevention and detection measures are in place at all premises from which the Service is provided or managed.
2.11.12	The Supplier must ensure that all ICT systems are secured appropriately to the level of risk associated with the secure materials and data being held or processed on such systems, according to policies based on ISO/IEC 27001 and the HMG SPF currently.
2.11.13	The Supplier must ensure that all desk-top computers used by Supplier personnel delivering the Service are password-protected, lock automatically after 5 minutes of inactivity and that the use of removable media devices (CD writer, DVD writer, memory sticks and similar) is controlled or disabled, in compliance with Supplier's security policy and the HMG Security Policy Framework.
2.11.14	The Supplier must ensure that all data relating to the Application held on portable devices including laptops are securely encrypted, and cannot be accessed in the event of theft or loss.
2.11.15	The Supplier must ensure that all data relating to the Application held on the Supplier's network is secured. Data files and secure materials relating to the Application must be stored on network drives, not on local storage, and network drives must be located in a secure server room, with only approved systems administrators having access to the server room.

2.11.16	The Supplier will co-operate with STA at all times to allow access to Supplier premises and systems to allow assurance to take place that all plans policies and procedures are being complied with by the Supplier.
2.11.17	The Supplier shall evidence working towards compliance with Security Policy Framework minimum mandatory measures and shall ensure that controls are in place relevant to the Classification of STA Data.
2.11.18	The Supplier shall record compliance, and evidence of such compliance, using a self-assessment checklist satisfactory to STA and shall make available to STA an updated self-assessment check-list: (i) on or by the date for the security document and Business Continuity Plans to be complet-ed; and (ii) promptly following a change: • In the operational requirements of the National Curriculum Assessments; or • To one or more Security Policy Framework minimum mandatory measures.
2.12 Business Continuity	
2.12.1	The Supplier must provide a Business Continuity Plan (BCP) and Disaster Recovery Plan (DR) for STA's approval. In addition the BCP and DR must have been approved by the Supplier's board/executive. The BCP and DR must meet Cabinet Office SPF requirements and be aligned or certified to BS 25999 or ISO 22301. The Supplier must utilise the BCP and DR in the management of the service to ensure that there is no interruption or failure which puts successful delivery of the Service at risk, this should be achieved through the provision of failover service for the live environment.
2.12.2	The Supplier must ensure that the Application and associated data are backed up daily. As a minimum, the Supplier must provide a weekly full backup supplemented by a daily incremental backup. The Supplier must ensure that there are at least two copies of each backup.
2.12.3	The Supplier must ensure that one copy of each backup is held on-site, in a secure, fireproof safe.
2.12.4	The Supplier must ensure that one copy of each backup is held at an off-site location, in a secure, fireproof safe.
2.12.5	The Supplier must ensure that an appropriate media rotation procedure is followed, in line with ISO/IEC 27001 and Government security policies.
2.12.6	The Supplier shall ensure that the RPO (Recovery Point Objective) is no more than 24 hours and the RTO (Recovery Time Objective) is no more than 4 hours
2.13 Exit and Transition	
2.13.1	The Supplier will provide and maintain a detailed, fully resourced and costed Exit and Transition Plan to ensure the smooth transition of Services to a Successor Service Provider.
2.13.2	The Supplier will provide a detailed statement in the Exit and Transition Plan of all its requirements for the support it requires from STA to ensure smooth transition of Service to a Successor Service Provider at the expiry or termination of the Framework.
2.13.3	The Supplier will provide a full Warranty on the Application and associated documentation for a period of 6 months following expiry or termination of the contract.

ANNEX 1A – MOBILISATION

1. Mobilisation

1.1 The Supplier shall, at no cost to DfE, manage all aspects of Transition (for delivery of the services from the incumbent supplier) in accordance with clause S3-32 or similar methodologies agreed in advance with DfE. The Supplier shall ensure that there is no break in service in the provision of the Application during Transition.

1.2 The Supplier shall pre-populate the Application with data including data in relation to a school or a Local Authority as provided by DfE from time to time, and within such time and in such manner as specified by DfE. The Supplier shall propose and implement a solution acceptable to DfE to ensure that any data that cannot be uploaded and displayed correctly (for example long school names) is validly uploaded and displayed on the Application.

1.3 The Supplier shall submit a PID (project initiation document) to be agreed by DfE which clearly sets out the Transition project from the outset. This document shall be consistent with PRINCE2 (or similar) controls and cover all aspects of Transition (for delivery of the services) of the project. The PID shall be provided by the Supplier to DfE by 30th June 2017 or two weeks from Date of Order Form (whichever is the earliest).

1.4 The Supplier shall produce and maintain a service guide to be used by the Supplier and DfE's service management teams (the "Service Guide"), within 1 month of the Effective Date. The Service Guide shall be written in layman's terms and contain the following sections:

1.4.1 Technical Overview

1.4.2 Incident Reporting and Management Procedures

1.4.3 Service Levels and Service Credits

1.4.4 Management Information and Reports

1.4.5 Change Management

1.4.6 Escalation Procedures and Key Contacts

1.5 The Supplier shall produce a Supplier Application Test Strategy and plan, for the approval of DfE, within 1 month of the Service Effective Date. During each change during the contract term, the Supplier shall ensure that the agreed test strategy and plan are adhered to for all aspects of their solution employed in delivering the Service. The test strategy and plan shall be reviewed for each change during the contract term. Where a change is to be made to the Application, the Supplier shall agree, with DfE, the scope of the testing for the changes and the associated Acceptance Criteria prior to any System development or testing taking place.

1.6 The Supplier shall provide an Application development strategy for agreement with DfE within 1 month of the Service Effective Date.

1.7 Software owned by DfE or developed by the Supplier in provision of the Services shall comply with open standards and shall be portable at the effective date of the expiry or termination of the Agreement.

1.8 The Supplier shall ensure that the following documentation is available, within three months of the Service Effective Date, for the Application (following transition and after any change to any of the applications) and describes the architecture and components in sufficient detail that any successor operator or users not involved in the initial development can use, install, operate and maintain the Application. This should include but not be limited to:

1.8.1 A design document with architectural diagrams describing the Application infrastructure;

1.8.2 Interface documentation containing details of interfaces between modules where information is shared and to any other external systems;

1.8.3 A technical specification document defining the technical aspects of the Application, including the standards to which they have adhered (noting that the Cabinet Office guidelines insist that procured solutions are based upon recognised open standards where they exist);

1.8.4 A functional specification document or equivalent defining the functional operation of the Application; and

1.8.5 Documentation of operation and user processes.

1.9 The Supplier shall put in place the necessary measures to keep this documentation up to date and available to DfE on request and in accordance with the Agreement.

2. Mobilisation Plan

2.1 The Supplier shall provide a Project Plan detailing the resources, tasks and timescales required to be performed for the Transition of the Services from previous contracts together with a summary milestone plan which details the deliverables outlined in the Project Initiation Document, and requirements / dependencies upon DfE. The Mobilisation Plan shall be provided by the Supplier to DfE by 17th August 2017 or two weeks from Date of Order Form (whichever is the earliest).

2.2 Within three month of the commencement of the contract the Supplier shall have produced:

2.2.1 A Security Document which has been agreed with DfE.

2.2.2 A Business Continuity Plan and Disaster Recovery Plan which has been agreed with DfE;

2.2.3 Agreed an initial Exit Plan and initial Exit Information Document with DfE;

2.2.4 Awarded contracts for any elements of the Service which shall be delivered by Subcontractors; and

2.2.5 A Service Plan agreed with DfE.

The schedule for delivery of the above is contained in section 12.1 of the Order Form.

2.3 The Supplier shall discuss and demonstrate to DfE the readiness and appropriateness of plans, processes, systems, resourcing and any other factors required to enable the reliable completion of the work.

2.4 Plans shall be kept up-to-date by the Supplier and communicated to DfE weekly or as required.

ANNEX 1B – CUSTOMER ACCEPTANCE TESTS

1. Application Test Strategy

1.1 The Supplier shall submit for DfE's review and approval a draft supplier application test strategy document (the "Supplier Application Test Strategy Document"). Following DfE's review of such materials, the Supplier shall amend the Supplier Application Test Strategy Document in accordance with any recommendations by DfE, until such document is approved by DfE. [Note to Supplier: the expectation is that during mobilisation the Supplier Application Test Strategy Document shall be included as part of the Mobilisation Plan as at the Effective Date and it is expected that it will satisfy the requirements set out in this Schedule. This Schedule may be amended to reflect any such document]

1.2 The Supplier shall ensure that the Supplier Application Test Strategy Document includes:

1.2.1 an overview of how application testing shall be conducted, including details of testing with third parties, unit testing, link testing, component failure testing, system testing, regression testing, penetration testing, operational Acceptance Testing, user Acceptance Testing, load Acceptance Testing and accessibility Acceptance Testing;

1.2.2 for volume and stress testing, full details of the volumetric assumptions that the Application shall be tested against;

1.2.3 for penetration testing, the identity of a proposed independent third party Supplier to perform such penetration testing, provided that the final identity of such third party shall be subject to DfE's prior approval;

1.2.4 the supplier and DfE shall agree a plan to remediate the risks and issues identified in the penetration testing specified in 1.2.3 above.

1.2.5 a full description of the tools and methodologies to be used for each stage of Application Testing (e.g. the development and use of test harnesses, which shall include reusable and re-configurable code where possible);

1.2.6 the process to be used to capture and record Application Testing results and the categorisation of Application Testing issues;

1.2.7 the definition of the acceptance criteria to be used for each Application Test (which criteria the Supplier shall revise in accordance with DfE's requirements) (the "Acceptance Criteria");

1.2.8 the method for mapping the expected Application Test results to the Application Test success criteria;

1.2.9 the definition of the approach for Application Test case management;

1.2.10 the process for capturing and managing Application Test defects, including the definition of Application Test defect levels (both severity and priority), and resolution times for defects (which shall be based on severity and priority). The Supplier shall keep the log of defects up to date, and make it available to DfE upon request;

1.2.11 details of how Application Test defect management reports shall be provided to DfE, such reports to be classified by severity and priority and include an issues log, fault, impact, RAG rating, corrective action and issue owner. The Supplier shall update these reports on a regular basis and make them available to DfE for review upon request;

1.2.12 the procedure to be followed in the event that the Application fails to satisfy the Acceptance Criteria or produces unexpected results, including a procedure for the resolution of Application Test issues;

1.2.13 the procedure to be followed to sign off each Application Test;

1.2.14 the procedure to be followed for signing off interfaces with third party systems;

1.2.15 the process for the production and maintenance of Application Test reports and reporting of progress and quality to DfE (including templates for the Application Test reports and the Application Test defect management log, and a sample plan to resolve Application Test defects);

1.2.16 the names and contact details of key Application Test-related contacts from each of the organisations involved in the Application Tests;

1.2.17 a high-level identification of the resources required for the Application Tests, including facilities, infrastructure, personnel and DfE's and/or third party involvement in the conduct of the Application Tests;

1.2.18 a description of the technical environments defined to support the Application Tests;

1.2.19 a description of the procedure for managing the configuration of the Application Test environments, including any tools for the Application Tests;

1.2.20 a description of the arrangements for allowing DfE to inspect Application Test results or witness the Application Tests in order to establish that the success criteria have been met and best practices have been followed; and

1.2.21 a description of the procedure for allowing a DfE representative to confirm the classification of any Application Test defects unresolved at the end of an Application Test in consultation with the Supplier.

1.3 The Supplier and DFE shall agree the scope of Application Tests in proportion to, and taking account of, the complexity of the change being requested.

1.4 The Supplier shall perform the Application Tests for the Services in compliance with the Supplier Application Test Strategy Document approved by DfE. The Application Tests for the Services include the tests to be carried out to determine: (i) the completion of the Mobilisation Plan and any Development Services; and (ii) the outcome of the business continuity testing.

2. Test Plans

2.1 The Supplier shall, in respect of each Application Test, develop a test plan for DfE's approval ("Test Plan"). Following DfE's review of such plans, the Supplier shall amend the Test Plans in accordance with any recommendations by DfE, until such plans are approved by DfE.

2.2 The Supplier shall ensure that each Test Plan clearly shows the components of the Application that are subject to Application Tests and under what conditions those components are being tested.

2.3 Each Test Plan submitted by the Supplier shall include as a minimum:

2.3.1 the definition and the purpose of the relevant Application Test;

2.3.2 the specific success criteria to be met for the relevant Application Test;

2.3.3 a set of traceable requirements to which the Application Test can be linked;

2.3.4 full details of the start and end points/boundaries of each Application Test, including the inputs, outputs and details of the expected outcome;

2.3.5 a timetable for the Application Tests, including start and end dates;

2.3.6 details of the mechanism for Application Tests (including details of the way in which the Application Tests are carried out, including use of any tools);

2.3.7 full details of the tools used for the Application Tests and of the technical environment in which the Application Tests are performed;

2.3.8 the means for ensuring the quality, completeness and relevance of the Application Tests;

2.3.9 the process by which DfE shall ensure that any changes made to the Application as a result of Application Test results comply with the Change Control Procedure;

2.3.10 the re-test procedure (namely the timetable and the resources (including any third party involvement) which would be required for re-testing).

3. Co-operation in relation to Application Test Assurance

3.1 The Supplier shall carry out and be responsible for all Application Tests for the Application (including supporting Application Tests for the integration of systems with third party systems). The Supplier shall provide DfE and any DfE Service Providers with full co-operation in connection with any integration Application Tests.

3.2 The Supplier shall provide DfE with all reasonable information and assistance requested by DfE in order for DfE to carry out its own internal assurance procedures. Such assistance shall include completing any Application Test assurance checklists used by DfE to provide internal assurance to DfE stakeholders regarding Acceptance Tests. The Supplier shall allow DfE access to visit its site and inspect development and Acceptance Test procedures. In particular, the Supplier shall allow DfE to conduct assurance visits at any premises of the Supplier or its Subcontractors from which the Services are being delivered, for up to half a day per week during the period(s) in which Application Tests are being carried out.

4. Standard Application Tests

4.1 The following standard Acceptance Tests shall be carried out by the Supplier in a test environment on each occasion on which the Supplier believes that it has completed the Mobilisation Plan or a Development Service:

4.1.1 "Supplier Tests", comprising Application Testing undertaken by the Supplier at the Supplier's premises; and then once the Supplier Tests have been passed successfully -

4.1.2 "First UAT", comprising User Acceptance Testing undertaken remotely by DfE technical personnel nominated by DfE; and then once the First UAT has been passed successfully -

4.1.3 "Second UAT", comprising User Acceptance Testing undertaken remotely by DfE programme personnel, including business owners and senior stakeholders nominated by DfE; and then once the Second UAT has been passed successfully -

4.1.4 "Third UAT", comprising User Acceptance Testing undertaken remotely by a number of different Users nominated by DfE.

4.2 The Supplier shall make available to those persons undertaking the user Application Testing for the First UAT, Second UAT and Third UAT:

4.2.1 remote access to the Application in a test environment; and

4.2.2 any test scripts that DfE requests from time to time.

5. Application Testing

5.1 The Supplier shall provide DfE and any DfE Service Providers with full co-operation in connection with any Application Testing of the Application required by DfE from time to time. Such end-to-end testing shall include a full trial of data flows through component modules, test interfaces and possible failure scenarios.

6. Application Test Environments

6.1 In addition to the live environment, the Supplier shall provide a user acceptance testing environment on an on-going basis. No disaster recovery capability is required for the user acceptance testing environment. The Supplier shall ensure that the existence of this environment does not represent any additional security risk for the live environment.

ANNEX 1C – SERVICE MANAGEMENT, SERVICE LEVELS AND SERVICE CREDITS

1. Service Management

1.1 The Supplier shall ensure that its approach to Service Management is aligned with ITIL version 3.

1.2 The reference for all ITIL related references in this section can be found at:

http://www.itil-officialsite.com

2. Capacity Management

2.1 The Supplier shall document (and agree with DfE) its approach to Capacity Management which shall align with ITIL version 3.

2.2 The Supplier shall develop a Capacity Plan to demonstrate how the Supplier shall manage identified patterns of business activity and the potential for growth of users and data over the contract term if, for example, key stage 4 schools were given access to the system following a policy decision.

3. Change and Release Management

3.1 The Supplier shall document (and agree with DfE) its approach to Change and Release management process which shall align with ITIL version 3.

3.2 The Supplier's Change and Release management process documentation should include (at a minimum):

3.2.1 Details of change windows;

3.2.2 Details of pre-planned outages; and

3.2.3 Release schedules.

3.3 The Supplier shall ensure that any change to the Application is authorised by DfE.

4. Incident and Problem Management

4.1 The Supplier shall document (and agree with DfE) its approach to Incident and Problem Management which shall align with ITIL version 3.

4.2 The Supplier shall be responsible for the resolution of all Incidents and Problems that are raised by DfE.

5. Service Reporting

5.1 The Supplier shall document (and agree with DfE) its approach to Service reporting which shall align with ITIL version 3.

5.2 The Supplier shall provide Service Management reports to DfE in advance and in line with its existing Service Management requirements which currently utilise a monthly service report cycle. Additionally the Service reports shall be made available to DfE on request.

5.3 The Service reports shall include, but not be limited to, a management summary and detailed breakdown including:

5.3.1 Availability / non availability;

5.3.2 Incidents and Problems raised, resolved and outstanding;

5.3.3 Impact assessments;

5.3.4 Minor enhancements;

5.3.5 Risks and issues;

5.3.6 Performance against Service Levels;

5.3.7 Forward plans;

5.3.8 Service metrics; and

5.3.9 Service call response times and any target breaches.

6. Configuration Management

6.1 The Supplier shall put an effective and appropriate configuration management procedure in place in accordance with Good Industry Practice, to establish and ensure the consistency of the Application's performance and its functional and physical attributes and conformance with the Application Requirements and operational characteristics during the term of the Agreement.

7. Service Levels

Application Availability

7.1 The Supplier shall host the Application on a domain or sub-domain as specified by DfE.

7.2 The Supplier shall provide sufficient bandwidth for the Application to ensure that the Application functions efficiently. The Application shall show no degradation of services where usage is equal to or below 120% of the maximum estimated concurrent users (circa 1,000). The Supplier shall be able to produce performance testing data verifying bandwidth usage.

7.3 The Supplier shall ensure that the Application is Available 24 hours a day with an Availability of at least 99.8%. The Availability shall be calculated on a monthly basis and shall exclude any Scheduled Maintenance.

7.4 For the purposes of this paragraph "**Available**" and "**Availability**" mean that:

7.4.1 the Application is capable of accepting and processing incoming requests and data and responding to hyperlinks within pages; and

7.4.2 Users can view all of the pages on the Application from the public internet in accordance with the Mandatory Requirements. Availability is measured at the point at which the Application interfaces with the public internet.

7.5 Availability shall not include periods of planned Routine Maintenance which shall be agreed in advance with DfE.

7.6 For Application Availability, the percentage availability shall be calculated over a calendar month using the following equation:

(B-A)/B*100=AVAILABILITY%

Where:

A – Total amount of time (in minutes) that the Application was not Available during the relevant calendar month

B – Total amount of time (in minutes) in the relevant calendar month excluding the total amount of time (in minutes) that the Application was not Available as a result of Scheduled Maintenance.

e.g. if a month has 31 days and the Application is not Available for 30 minutes, with 10 minutes of Scheduled Maintenance, then the percentage availability shall be calculated as:

A=30, B= (31*1440)-10=44630

(44630-30)/44630*100=99.93%

7.7 The Supplier shall ensure that it puts in place the necessary infrastructure to ensure that the automated uploads of data by DfE are supported for all current functionality.

7.8 The supplier shall provide a duplicate of the live environment which is available to STA throughout the year. The Test Environment shall be Available for a minimum of 95% during the hours of 7am to 7pm, Monday to Friday. There may be a requirement to utilise the Test Environment out of these hours and DfE should be informed if there are any planned outages of the Test Environment.

8. Scheduled Maintenance

8.1 Any maintenance carried out by the Supplier in accordance with this paragraph shall be known as "**Scheduled Maintenance**".

8.2 The Supplier shall ensure that all Scheduled Maintenance is carried out during a daily window of 12am to 4am. The Supplier shall notify DfE of any Scheduled Maintenance required to be undertaken outside this window and the reason for the maintenance at least 10 working days in advance of the maintenance being performed.

8.3 The Supplier shall notify DfE if any emergency maintenance is to be undertaken and the reason for the emergency maintenance, which cannot be carried out without the agreement of DfE. Any Emergency Maintenance performed outside of the Scheduled Maintenance window will count as downtime for the calculation of availability. Emergency Maintenance will include the application of any critical security patches that are required to protect the service.

8.4 The Supplier shall produce, agree with DfE and maintain a rolling schedule of time windows during which Scheduled Maintenance may be carried out in respect of the Application with minimum disruption to Users ("**Scheduled Maintenance Windows**").

8.5 The Supplier shall ensure that, unless otherwise agreed with DfE in writing, the total time allocated for Scheduled Maintenance Windows does not exceed: (a) 18 hours in any successive three month period; or (b) eight hours in any calendar month.

8.6 The Supplier shall ensure that all non-critical patches for system components, as well as hardware and software updates and upgrades, are carried out during Scheduled Maintenance Windows.

8.7 The Supplier shall answer any questions DfE may have regarding the impact that an update or upgrade may have on security compliance promptly, and in any event within one Business Day of receiving such request.

8.8 Except in respect of emergency maintenance, the Supplier shall ensure that any maintenance relating to the Application:

8.8.1 is carried out within the Scheduled Maintenance Windows or as otherwise agreed with DfE with at least 10 Business Days' prior written notice;

8.8.2 is carried out during times not falling within the Core Hours;

8.8.3 is entered on to the maintenance schedule (including a description of the maintenance carried out, the time it was carried out and the reason for its being carried out); and

8.8.4 is not carried out during the peak activity periods, as notified by DfE to the Supplier in accordance with clause 13.1 (Response Times).

9. Technical Helpdesk Availability

9.1 The Supplier shall ensure that the Technical Helpdesk is available during the following times: 08.30 to 17.30 during weekdays, excluding Bank holidays.

9.2 During July, the Supplier shall provide an out of hours technical support service to ensure the delivery of Return of Results.

9.3 The Supplier shall ensure that the Helpdesk has a minimum 99% Availability.

9.4 The Supplier shall ensure that the Helpdesk shall not remain un-Available for more than 15 minutes in any one continuous period during the Core Hours.

9.5 If the Supplier fails to provide the Services in accordance with the Service Levels then Service Credits shall become payable by the Supplier in accordance with paragraph clause 12 below.

9.6 For the purposes of this clause 9, “Available” and “Availability” mean that: (i) the Helpdesk is fully operational with live agents that deal with all enquiries in English within 15 seconds of the point at which the call is made.

9.7 For Helpdesk Availability, the percentage availability shall be calculated over a calendar month using the following equation:

(B-A)/B*100=AVAILABILITY%

Where:

A – Total amount of time (in minutes) that the Helpdesk was not Available during the relevant calendar month

B – Total amount of time (in minutes) in the relevant calendar month.

e.g. if a month has 31 days and the Helpdesk is not Available for 30 minutes, then the percentage availability shall be calculated as:

A=30, B=(31*1440)=44640

(44640-30)/44640*100=99.93%

9.8 DfE’s Helpdesk may report faults to the Supplier relating to the Application by calling the Supplier by telephone or by email.

10. Transaction Times

10.1 The Supplier shall ensure that the Application delivers an average Transactional Response Time of no greater than 2 seconds to the perimeter of systems within the Supplier's network. The transaction shall be measured from the time the Supplier receives the instruction to perform the transaction and is delivered to the perimeter of the systems within the Supplier's network. The average shall be calculated over a monthly period.

10.2 Transactional operations include the submission of applications and the retrieval and display of data.

10.3 The Supplier shall ensure that the Application delivers an average non-Transactional Response Time of no greater than 1 second to the perimeter of systems within the Supplier's network. The transaction shall be measured from the time the Supplier receives the instruction to perform the transaction and is delivered to the perimeter of the systems within the Supplier's network. The average shall be calculated over a monthly period.

10.4 Non-transaction operations include the display of help text, menus and other navigational assets.

11. Response Times

11.1 For the purposes of this paragraph “**Peak Period**” means the following periods:

October 31st to November 25th;

February 1st to May 31st

June 20th to July 29th

September 5th to September 16th

For the avoidance of doubt any peak Period shall start on the Monday closest to the start of the period and end on the Friday closest to the end of the period. These are indicative Peak Period dates and DfE will agree with the Supplier the exact dates each year.

11.2 The Supplier shall categorise each Incident and Problem and provide DfE with the category and proposed time for resolution.

11.3 The Supplier shall respond to incidents and requests that are raised by DfE in accordance with the response times set out in Schedule 2 of The Supplier's Terms and Conditions.

12. Service Credits

12.1 If the Supplier fails to provide the Services in accordance with the Service Levels set out in paragraphs 8 (Application Availability), 6 (Technical Helpdesk) and 13 (Response Times) then Service Credits shall become payable by the Supplier as set out in this paragraph.

12.2 Each Service Level has a number of Service Points set against it in the table below, which shall be awarded to DfE if the Supplier fails to achieve the relevant Service Level.

12.3 The value of a Service Point shall be calculated as follows: 1 Service Point = 0.5% of the total monthly Charges.

12.4 In any month: Service Credit = total Service Points awarded to DfE * value of 1 Service Point.

Service Level	**Increment**	**Service Points**	**Notes**
Application Availability	For every 0.1% of Availability below the Service Level in paragraph 7 (Application Availability)	2 Service Points shall apply during Core Hours 1 Service Point shall apply at other times	Measured monthly
Helpdesk Availability	For every 0.1% of Availability below Service Level in paragraph 9 (Helpdesk Availability)	1 Service Point shall apply	Measured monthly
Response Times	For every failure to meet a Response Time Service Level in paragraph 11 (Response Times)	2 Service Points shall apply to a failure to meet Priority Level P1 Response Times 1 Service Point shall apply to any failure to meet all other Priority Level Response Times 1 Service Point shall apply where updates on progress are required for Priority Level P1 Response Times and the Supplier fails to provide such updates	

G-CLOUD SERVICES CALL-OFF TERMS

The Department for Education of Sanctuary Buildings, Great Smith Street, London, SW1P 3BT (the "**Customer**"); - and

The Stationery Office Limited, a company registered in England under company number 03049649 and whose registered office is at 29 St. John's Lane, London, EC1M 4NA (the "**Supplier**").

relating to

the provision of G-Cloud Services.

CALL-OFF AGREEMENT TERMS AND CONDITIONS

THIS CONTRACT is made on the 19th day of May 2017

BETWEEN

(1) The Department for Education of Sanctuary Buildings, Great Smith Street, London, SW1P 3BT (the "**Customer**"); and

(2) The Stationery Office Limited, a company registered in England under company number 03049649 and whose registered office is at 29 St. John's Lane, London, EC1M 4NA (the "**Supplier**").

IT IS AGREED AS FOLLOWS:

CO-1 OVERRIDING PROVISIONS

CO-1.1 The Supplier agrees to supply the G-Cloud Services and any G-Cloud Additional Services in accordance with the Call-Off Terms, including Supplier's Terms as identified in Framework Schedule 1 (G-Cloud Services) and incorporated into this Call-Off Agreement.

CO-1.2 In the event of and only to the extent of any conflict or ambiguity between the Clauses of this Call-Off Agreement, the provisions of the Schedules, any document referred to in the Clauses of this Call-Off Agreement (including Supplier's Terms) and the Framework Agreement, the conflict shall be resolved in accordance with the following order of precedence:

CO-1.2.1 the Framework Agreement (excluding Framework Schedule 2);

CO-1.2.2 the Clauses of this Call-Off Agreement (excluding Supplier Terms);

CO-1.2.3 the completed Order Form;

CO-1.2.4 the DfE Special Terms;

CO-1.2.5 the Supplier's Terms as set out in the Framework Schedule 1 (G-Cloud Services); and

CO-1.2.6 any other document referred to in the Clauses of this Call-Off Agreement.

CO-1.3 The Supplier acknowledges and accepts that the order of prevailing provisions in this Call-Off Agreement is as set out in Clause CO-1.2 above.

CO-2 PREVENTION OF BRIBERY AND CORRUPTION

CO-2.1 If the Supplier breaches

CO-2.1.1 Clauses FW-22.1 or FW-22.2 of the Framework Agreement; or,

CO-2.1.2 the Bribery Act 2010 in relation to the Framework Agreement

CO-2.1.3 the Customer may terminate this Call-Off Agreement.

CO-2.2 The Parties agree that the Management Charge payable in accordance with Clause FW-9 does not constitute an offence under section 1 of the Bribery Act 2010.

CO-3 PROTECTION OF INFORMATION

CO-3.1 The provisions of this Clause CO-3, shall apply during the Call-Off Agreement Period and for such time as the Supplier holds the Customer Personal Data.

CO-3.2 The Supplier shall and shall procure that Supplier's Staff comply with any notification requirements under the DPA and both Parties undertake to duly observe all their obligations under the DPA which arise in connection with the Call-Off Agreement.

CO-3.3 To the extent that the Supplier is Processing the Order Personal Data the Supplier shall:

CO-3.3.1 ensure that it has in place appropriate technical and organisational measures to ensure the security of the Order Personal Data (and to guard against unauthorised or unlawful Processing of the Order Personal Data and against accidental loss or destruction of, or damage to, the Order Personal Data; and

CO-3.3.2 provide the Customer with such information as the Customer may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA;

CO-3.3.3 promptly notify the Customer of any breach of the security measures to be put in place pursuant to this Clause; and

CO-3.3.4 ensure that it does not knowingly or negligently do or omit to do anything which places the Customer in breach of its obligations under the DPA.

CO-3.4 To the extent that the Supplier Processes Service Personal Data the Supplier shall:

CO-3.4.1 Process Service Personal Data only in accordance with written instructions from the Customer as set out in this Call-Off Agreement;

CO-3.4.2 Process the Service Personal Data only to the extent, and in such manner, as is necessary for the provision of the G-Cloud Services or as is required by Law or any Regulatory Body;

CO-3.4.3 implement appropriate technical and organisational measures to protect Service Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to Service Personal Data and having regard to the nature of the Service Personal Data which is to be protected;

CO-3.4.4 take reasonable steps to ensure the reliability of any Supplier Staff who have access to Service Personal Data;

CO-3.4.5 ensure that all Supplier Staff required to access Service Personal Data are informed of the confidential nature of the Service Personal Data and comply with the obligations set out in this Clause;

CO-3.4.6 ensure that none of the Supplier Staff publish, disclose or divulge Customer's Personal Data to any third party unless necessary for the provision of the G-Cloud Services under the Call-Off Agreement and/or directed in writing to do so by the Customer;

CO-3.4.7 notify the Customer within five (5) Working Days if it receives:

CO-3.4.7.1 a request from a Data Subject to have access to Service Personal Data relating to that person; or

CO-3.4.7.2 a complaint or request relating to the Customer's obligations under the Data Protection Legislation;

CO-3.4.8 provide the Customer with full cooperation and assistance in relation to any complaint or request made relating to Service Personal Data, including by:

CO-3.4.8.1 providing the Customer with full details of the complaint or request;

CO-3.4.8.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Customer's instructions;

CO-3.4.8.3 providing the Customer with any Service Personal Data it holds in relation to a Data Subject (within the timescales required by the Customer); and

CO-3.4.8.4 providing the Customer with any information requested by the Data Subject.

CO-3.5 The Supplier shall:

CO-3.5.1 permit the Customer or the Customer's Representative (subject to the reasonable and appropriate confidentiality undertakings), to inspect and audit the Supplier's data Processing activities (and/or those of its agents, subsidiaries and Sub-Contractors) or provide to the Customer an independent third party inspection and audit certificate in lieu of the same (unless otherwise agreed between the Parties, the option of providing a certificate in lieu shall not be available at IL3 and above) and shall comply with all reasonable requests or directions by the Customer to enable the Customer to verify and/or procure that the Supplier is in full compliance with its obligations under this Call-Off Agreement; and/or

CO-3.5.2 subject to Clause CO-3.6 agree to an appointment of an independent auditor selected by the Supplier to undertake the activities in Clause CO-3.5.1 provided such selection is acceptable to the Customer or Customer Representative (subject to such independent auditor complying with the reasonable and appropriate confidentiality undertakings).

CO-3.6 The Supplier Shall:

CO-3.6.1 obtain prior written consent from the Customer in order to transfer Customer Personal Data to any other person (including for the avoidance of doubt any Sub-Contractors) for the provision of the G-Cloud Services;

CO-3.6.2 not cause or permit to be Processed, stored, accessed or otherwise transferred outside the EEA any Customer Personal Data supplied to it by the Customer without the prior written consent of the Customer. Where the Customer consents to such Processing, storing, accessing or transfer outside the European Economic Area the Supplier shall:

CO-3.6.3 comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is so processed, stored, accessed or transferred;

CO-3.6.4 comply with any reasonable instructions notified to it by the Customer and either:

CO-3.6.5 incorporate standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) or warrant that that the obligations set out in the Supplier Terms provide Adequate protection for Personal Data.

CO-3.7 The Supplier shall not perform its obligations under this Call-Off Agreement in such a way as to cause the Customer to breach any of its applicable obligations under the Data Protection Legislation.

CO-3.8 The Supplier acknowledges that, in the event that it breaches (or attempts or threatens to breach) its obligations relating to Customer Personal Data that the Customer may be irreparably harmed (including harm to its reputation). In such circumstances, the Customer may proceed directly to court and seek injunctive or other equitable relief to remedy or prevent any further breach (or attempted or threatened breach).

CO-4 CONFIDENTIALITY

CO-4.1 Except to the extent set out in this Clause or where disclosure is expressly permitted elsewhere in this Call-Off Agreement, each Party shall:

CO-4.1.1 treat the other Party's Confidential Information as confidential and safeguard it accordingly; and

CO-4.1.2 not disclose any Confidential Information belonging to the other Party to any other person without the prior written consent of the other Party, except to such persons and to such extent as may be necessary for the performance of this Call-Off Agreement.

CO-4.2 The Supplier may only disclose the Customer's Confidential Information to the Supplier Staff who are directly involved in the provision of the G-Cloud Services and who need to know the information, and shall ensure that such Supplier Staff are aware of and shall comply with these obligations as to confidentiality.

CO-4.3 The Supplier shall not, and shall procure that the Supplier Staff do not, use any of the Customer's Confidential Information received otherwise than for the purposes of this Call-Off Agreement.

CO-4.4 The provisions of Clauses CO-4.1 shall not apply to the extent that:

CO-4.4.1 such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under Clause CO-7 (Transparency) and the FOIA, the Ministry of Justice Code or the Environmental Information Regulations pursuant to Clause CO-6 (Freedom of Information);

CO-4.4.2 such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

CO-4.4.3 such information was obtained from a third party without obligation of confidentiality;

CO-4.4.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Call-Off Agreement; or

CO-4.4.5 it is independently developed without access to the other Party's Confidential Information.

CO-4.5 Nothing in this Call-Off Agreement shall prevent the Customer from disclosing the Supplier's Confidential Information (including the Management Information obtained under Clause FW-8 (Provision of Management Information) of the Framework Agreement):

CO-4.5.1 for the purpose of the examination and certification of the Customer's accounts;

CO-4.5.2 for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Customer has used its resources;

CO-4.5.3 to any Crown body or any Other Contracting Body. All Crown bodies or Contracting Bodies receiving such Supplier's Confidential Information shall be entitled to further disclose the Supplier's Confidential Information to other Crown bodies or Other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown body or any Contracting Body; or

CO-4.5.4 to any consultant, contractor or other person engaged by the Customer (on the basis that the information shall be held by such consultant, contractor or other person in confidence and is not to be disclosed to any third party) or any person conducting a Cabinet Office or ERG Gateway review or any additional assurance programme.

CO-4.6 In the event that the Supplier fails to comply with Clauses CO-4.1 to Clause CO-4.4, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by notice in writing.

CO-4.7 In order to ensure that no unauthorised person gains access to any Confidential Information or any data obtained in performance of this Call-Off Agreement, the Supplier undertakes to maintain adequate security arrangements that meet the requirements of Good Industry Practice.

CO-4.8 The Supplier will immediately notify the Customer of any breach of security in relation to Customer Confidential Information obtained in the performance of this Call-Off Agreement and will keep a record of such breaches. The Supplier will use its best endeavours to recover such Customer Confidential Information however it may be recorded. This obligation is in addition to the Supplier's obligations under Clauses CO-4.1 to Clause CO-4.4. The Supplier will co-operate with the Customer in any investigation that the Customer considers necessary to undertake as a result of any breach of security in relation to Customer Confidential Information.

CO-4.9 Subject always to Clause CO-11.4 the Supplier shall, at all times during and after the Call-Off Agreement Period, indemnify the Customer and keep the Customer fully indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against the Customer arising from any breach of the Supplier's obligations under the DPA or this Clause CO-4 (Confidentiality) except and to the extent that such liabilities have resulted directly from the Customer's instructions.

CO-5 CUSTOMER DATA

CO-5.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Customer Data.

CO-5.2 The Supplier shall not store, copy, disclose, or use the Customer Data except as necessary for the performance by the Supplier of its obligations under this Call-Off Agreement or as otherwise expressly approved by the Customer.

CO-5.3 The Supplier shall ensure that any system on which the Supplier holds any Customer Data, including back-up data, is a secure system that complies with the Supplier security policy.

STATUTORY OBLIGATIONS AND REGULATIONS

CO-6 FREEDOM OF INFORMATION

CO-6.1 The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and co-operate with the Customer to enable the Customer to comply with its Information disclosure obligations.

CO-6.2 The Supplier shall:

CO-6.2.1 transfer to the Customer all Requests for Information that it receives as soon as practicable and in any event within two (2) Working Days of receiving a Request for Information;

CO-6.2.2 provide the Customer with a copy of all Information, relating to a Request for Information, in its possession or control, in the form that the Customer requires within five (5) Working Days (or such other period as the Customer may specify) of the Customer's request; and

CO-6.2.3 provide all necessary assistance as reasonably requested by the Customer to enable the Customer to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

CO-6.3 The Customer shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Call-Off Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information (including Supplier’s Confidential Information) is

exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.

CO-6.4 In no event shall the Supplier respond directly to a Request for Information unless authorised in writing to do so by the Customer.

CO-6.5 The Supplier acknowledges that the Customer may, acting in accordance with the Ministry of Justice Code, be obliged under the FOIA, or the Environmental Information Regulations to disclose Information concerning the Supplier or the G-Cloud Services:

CO-6.5.1 in certain circumstances without consulting the Supplier; or

CO-6.5.2 following consultation with the Supplier and having taken its views into account;

provided always that where Clause CO-6.5.1 applies the Customer shall, in accordance with any recommendations of the Ministry of Justice Code, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

CO-6.5.3 The Supplier acknowledges that the description of information as Commercially Sensitive Information in Framework Schedule 6 (Interpretations and Definitions) is of an indicative nature only and that the Customer may be obliged to disclose it in accordance with this Clause CO-6.

CO-7 TRANSPARENCY

CO-7.1 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Call-Off Agreement is not Confidential Information. The Customer shall be responsible for determining in its absolute discretion whether any of the content of this Call-Off Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

CO-7.2 Notwithstanding any other term of this Call-Off Agreement, the Supplier hereby gives its consent for the Customer to publish this Call-Off Agreement in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted), including from time to time agreed changes to this Call-Off Agreement, to the general public.

CO-7.3 The Customer may consult with the Supplier to inform its decision regarding any redactions but the Customer shall have the final decision in its absolute discretion.

CO-7.4 The Supplier shall assist and cooperate with the Customer to enable the Customer to publish this Call-Off Agreement.

CO-8 OFFICIAL SECRETS ACTS

CO-8.1 The Supplier shall comply with and shall ensure that the Supplier Staff comply with, the provisions of:

CO-8.1.1 the Official Secrets Act 1911 to 1989; and

CO-8.1.2 Section 182 of the Finance Act 1989.

CO-8.2 In the event that the Supplier or the Supplier Staff fails to comply with this Clause, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by giving notice in writing to the Supplier.

CO-9 TERM AND TERMINATION

CO-9.1 This Call-Off Agreement shall take effect on the Effective Date and shall expire on:

CO-9.1.1 the date specified in paragraph 1.2 of the Order Form; or

CO-9.1.2 twenty four (24) Months after the Effective Date, whichever is the earlier, unless terminated earlier pursuant to this Clause CO-9.

CO-9.2 Termination without Cause

CO-9.2.1 The Customer shall have the right to terminate this Call-Off Agreement at any time by giving the length of written notice to the Supplier as set out in paragraph 10.2 of the Order Form.

CO-9.3 Termination on Change of Control

CO-9.3.1 The Supplier shall notify the Customer immediately if the Supplier undergoes a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 ("**Change of Control**") and provided this does not contravene any Law shall notify the Customer immediately in writing of any circumstances suggesting that a Change of Control is planned or in contemplation. The Customer may terminate the Call-Off Agreement by notice in writing with immediate effect within six (6) Months of:

CO-9.3.1.1 being notified in writing that a Change of Control has occurred or is planned or in contemplation; or

CO-9.2.1.2 where no notification has been made, the date that the Customer becomes aware of the Change of Control,

but shall not be permitted to terminate where a written approval was granted prior to the Change of Control.

CO-9.3.2 For the purposes of Clause CO-9.3.1, any transfer of shares or of any interest in shares by its affiliate company where such transfer forms part of a bona fide reorganisation or restructuring shall be disregarded.

CO-9.4 Termination by Supplier

CO-9.4.1 If the Customer fails to pay the Supplier undisputed sums of money when due, the Supplier shall notify the Customer in writing of such failure to pay and allow the Customer five (5) calendar days to settle undisputed invoice. If the Customer fails to pay such undisputed sums within allotted additional 5 calendar days, the Supplier may terminate this Call-Off Agreement subject to giving the length of notice as specified in paragraph 10.1 of the Order Form.

CO-9.5 Termination on Insolvency

CO-9.5.1 The Customer may terminate this Call-Off Agreement with immediate effect by notice in writing where the Supplier:

CO-9.5.1.1 being an individual, or where the Supplier is a firm, any partner or partners in that firm who together are able to exercise direct or indirect control, as defined by Section 416 of the Income and Corporation Taxes Act 1988, and:

CO-9.5.1.2 shall at any time become bankrupt or shall have a receiving order or administration order made against him or shall make any composition or arrangement with or for the benefit of his creditors, or shall make any conveyance or assignment for the benefit of his creditors, or shall purport so to do, or appears unable to pay or to have no reasonable prospect of being able to pay a debt within the meaning of Section 268 of the Insolvency Act 1986, or any similar event occurs under the law of any other jurisdiction; or

CO-9.5.1.3 a creditor or encumbrancer attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Supplier's assets and such

attachment or process is not discharged within fourteen (14) calendar days; or

CO-9.5.1.4 he dies or is adjudged incapable of managing his affairs within the meaning of Part VII of the Mental Health Act 1983; or

CO-9.5.1.5 the Supplier suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business.

CO-9.5.2 being a company, passes a resolution, or the Court makes an order that the Supplier or its Parent Company be wound up otherwise than for the purpose of a bona fide reconstruction or amalgamation, or a receiver, manager or administrator on behalf of a creditor is appointed in respect of the business or any part thereof of the Supplier or its Parent Company (or an application for the appointment of an administrator is made or notice to appoint an administrator is given in relation to the Supplier or its Parent Company), or circumstances arise which entitle the Court or a creditor to appoint a receiver, manager or administrator or which entitle the Court otherwise than for the purpose of a bona fide reconstruction or amalgamation to make a winding-up order, or the Supplier or its Parent Company is unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986 (except where the claim is made under Section 123(1)(a) and is for an amount of less than ten thousand pounds (£10,000)) or any similar event occurs under the law of any other jurisdiction.

CO-9.6 Termination on Material Breach

CO-9.6.1 The Customer may terminate this Call-Off Agreement with immediate effect by giving written notice to the Supplier if the Supplier commits a Material Breach of any obligation under this Call-Off Agreement and if:

CO-9.6.1.1 the Supplier has not remedied the Material Breach within thirty (30) Working Days (or such other longer period as may be specified by the Customer) of written notice to the Supplier specifying the Material Breach and requiring its remedy; or

CO-9.6.1.2 the Material Breach is not, in the opinion of the Customer capable of remedy.

CO-9.7 Termination for repeated Default

CO-9.7.1 If there are two or more Defaults (of a similar nature) that will be deemed a breach for Material Breach. Where the Customer considers that the Supplier has committed a repeated Default in relation to this Call-Off Agreement or any part thereof (including any part of the G-Cloud Services) and believes that the Default is remediable, then the Customer shall be entitled to serve a notice on the Supplier:

CO-9.7.1.1 specifying that it is a formal warning notice;

CO-9.7.1.2 giving reasonable details of the breach; and

CO-9.7.1.3 stating that such breach is a breach which, if it recurs or continues, may result in a termination of this Call-Off Agreement or that part of the G-Cloud Services affected by such breach.

CO-9.7.2 If, thirty (30) Working Days after service of a formal warning notice as described in Clause CO-9.7, the Supplier has failed to demonstrate to the satisfaction of the Customer that the breach specified has not continued or recurred and that the Supplier has put in place measures to ensure that such breach does not recur, then the Customer may deem such failure to be a Material Breach not capable of remedy for the purposes of Clause CO-9.6.1.2.

CO-9.8 The termination (howsoever arising) or expiry of this Call-Off Agreement pursuant to this Clause 9 shall be without prejudice to any rights of either the Customer or the Supplier that shall have accrued before the date of such termination or expiry.

CO-9.9 Save as aforesaid, the Supplier shall not be entitled to any payment from the Customer after the termination (howsoever arising) or expiry of this Call-Off Agreement.

CO-10 CONSEQUENCES OF SUSPENSION, TERMINATION AND EXPIRY

CO-10.1 Where a Customer has the right to terminate a Call-Off Agreement, it may elect to suspend this Call-Off Agreement and its performance.

CO-10.2 Notwithstanding the service of a notice to terminate this Call-Off Agreement or any part thereof, the Supplier shall continue to provide the Ordered G-Cloud Services until the date of expiry or termination (howsoever arising) of this Call-Off Agreement (or any part thereof) or such other date as required under this Clause CO-10.

CO-10.3 Within ten (10) Working Days of the earlier of the date of expiry or termination (howsoever arising) of this Call-Off Agreement, the Supplier shall return (or make available) to the Customer:

CO-10.3.1 any data (including (if any) Customer Data), Customer Personal Data and Customer Confidential Information in the Supplier's possession, power or control, either in its then current format or in a format nominated by the Customer (in which event the Customer will reimburse the Supplier's pre-agreed and reasonable data conversion expenses), together with all training manuals, access keys and other related documentation, and any other information and all copies thereof owned by the Customer, save that it may keep one copy of any such data or information for a period of up to twelve (12) Months to comply with its obligations under the Framework Schedule FW-5, or such period as is necessary for such compliance (after which time the data must be deleted); and

CO-10.3.2 any sums prepaid in respect of Ordered G-Cloud Services not provided by the date of expiry or termination (howsoever arising) of this Call-Off Agreement.

CO-10.4 The Customer and the Supplier shall comply with the exit and service transfer arrangements as per the Supplier's terms and conditions identified in Framework Schedule 1 (G-Cloud Services).

CO-10.5 Subject to Clause CO-11 (Liability), where the Customer terminates this Call-Off Agreement under Clause CO-9.2 (Termination without Cause), the Customer shall indemnify the Supplier against any reasonable and proven commitments, liabilities or expenditure which would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Call-Off Agreement, provided that the Supplier takes all reasonable steps to mitigate such loss. Where the Supplier holds insurance, the Supplier shall reduce its unavoidable costs by any insurance sums available. The Supplier shall submit a fully itemised and costed list of such loss, with supporting evidence, of losses reasonably and actually incurred by the Supplier as a result of termination under Clause CO-9.2 (Termination without Cause).

CO-11 LIABILITY

CO-11.1 Nothing in this Clause CO-11 shall affect a Party's general duty to mitigate its loss.

CO-11.2 Nothing in this Call-Off Agreement shall be construed to limit or exclude either Party's liability for:

CO-11.2.1 death or personal injury caused by its negligence or that of its staff;

CO-11.2.2 bribery, Fraud or fraudulent misrepresentation by it or that of its staff;

CO-11.2.3 any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982; or

CO-11.2.4.any other matter which, by Law, may not be excluded or limited.

CO-11.3 Nothing in this Call-Off Agreement shall impose any liability on the Customer in respect of any liability incurred by the Supplier to any other person, but this shall not be taken to exclude or limit any liability of the Customer to the Supplier that may arise by virtue of either a breach of the Call-Off Agreement or by negligence on the part of the Customer, or the Customer's employees, servants or agents.

CO-11.4 Subject always to Clause CO-11.2, the aggregate liability of either Party under or in connection with each Year of this Call-Off Agreement (whether expressed as an indemnity or otherwise):

CO-11.4.1 for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to the Customer Personal Data or Customer Data) of the other Party, shall be subject to the financial limits set out in paragraph 8.1 of the Order Form;

CO-11.4.2 and in respect of all other defaults, claims, losses or damages, whether arising from breach of contract, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall not exceed a sum equivalent to the financial limit set out in paragraph 8.3 of the Order Form .

CO-11.5 Subject always to Clause CO-11.4 the Customer shall have the right to recover as a direct loss:

CO-11.5.1 any additional operational and/or administrative expenses arising from the Supplier's Default;

CO-11.5.2 any wasted expenditure or charges rendered unnecessary and/or incurred by the Customer arising from the Supplier's Default; and

CO-11.5.3 any losses, costs, damages, expenses or other liabilities suffered or incurred by the Customer which arise out of or in connection with the loss of, corruption or damage to or failure to deliver Customer Data by the Supplier.

CO-11.6 The Supplier shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Call-Off Agreement.

CO-11.7 Subject to Clauses CO-11.2 and Clause CO-11.5, in no event shall either Party be liable to the other for any:

CO-11.7.1 loss of profits;

CO-11.7.2 loss of business;

CO-11.7.3 loss of revenue;

CO-11.7.4 loss of or damage to goodwill;

CO-11.7.5 loss of savings (whether anticipated or otherwise); and/or

CO-11.7.6 any indirect, special or consequential loss or damage.

CO-11.8 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall be subject to the financial limits set out in paragraph 8.2 of the Order Form.

CO-12 INSURANCE

CO-12.1 The Supplier shall effect and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the

Supplier, arising out of the Supplier's performance of its obligations under this Call-Off Agreement, including death or personal injury, loss of or damage to property or any other loss (including the insurance policies specified in the relevant paragraph of the Order Form). Such policies shall include cover in respect of any financial loss arising from any advice given or omitted to be given by the Supplier. Such insurance shall be maintained for the Call-Off Agreement Period and for the minimum insurance period as set out in paragraph 9 of the Order Form.

CO-12.2 The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under this Call-Off Agreement.

CO-13 PAYMENT, VAT AND CALL-OFF AGREEMENT CHARGES

CO-13.1 In consideration of the Supplier's performance of its obligations under this Call-Off Agreement, the Customer shall pay the Charges in accordance with the Clause CO-13.2 to CO-13.8.

CO-13.2 The Customer shall pay all sums properly due and payable to the Supplier in cleared funds within the time period specified in paragraph 6 of the Order Form.

CO-13.3 The Supplier shall ensure that each invoice contains all appropriate references and a detailed breakdown of the G-Cloud Services supplied and that it is supported by any other documentation reasonably required by the Customer to substantiate the invoice.

CO-13.4 Where the Supplier enters into a Sub-Contract it shall ensure that a provision is included in such Sub-Contract which requires payment to be made of all sums due by the Supplier to the Sub-Contractor within a specified period not exceeding thirty (30) calendar days from the receipt of a validly issued invoice, in accordance with the terms of the Sub-Contract.

CO-13.5 The Supplier shall add VAT to the Charges at the prevailing rate as applicable.

CO-13.6 The Supplier shall fully indemnify the Customer on demand and keep the Customer fully indemnified on a continuing basis against any liability, including without limitation against any interest, penalties or costs, which are suffered or incurred by or levied, demanded or assessed on the Customer at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Call-Off Agreement. Any amounts due under this Clause CO-13.6 shall be paid by the Supplier to the Customer not less than five (5) Working Days before the date upon which the tax or other liability is payable by the Customer.

CO-13.7 The Supplier shall not suspend the supply of the G-Cloud Services unless the Supplier is entitled to terminate this Call-Off Agreement under Clause CO-9.4 for Customer's failure to pay undisputed sums of money. Interest shall be payable by the Customer on the late payment of any undisputed sums of money properly invoiced in accordance with the Late Payment of Commercial Debts (Interest) Act 1998 (as amended from time to time).

CO-13.8 In the event of a disputed invoice, the Customer shall make payment in respect of any undisputed amount in accordance with the provisions of Clause CO-13 of this Call-Off Agreement and return the invoice to the Supplier within ten (10) Working Days of receipt with a covering statement proposing amendments to the invoice and/or the reason for any non-payment. The Supplier shall respond within ten (10) Working Days of receipt of the returned invoice stating whether or not the Supplier accepts the Customer's proposed amendments. If it does then the Supplier shall supply with the response a replacement valid invoice.

CO-13.9 The Supplier shall accept the Government Procurement Card as a means of payment for the G-Cloud Services where such card is agreed with the Customer to be a suitable means of payment. The Supplier shall be solely liable to pay any merchant fee levied for using the Government Procurement Card and shall not be entitled to recover this charge from the Customer.

CO-14 GUARANTEE

CO-14.1 Where the Customer has specified in the Order Form that this Call-Off Agreement shall be conditional upon receipt of a Guarantee from the guarantor, the Supplier shall deliver to the Customer an executed Guarantee from the guarantor, on or prior to the Commencement Date; and deliver to the Customer a certified copy of the passed resolution and/or board minutes of the guarantor approving the execution of the Guarantee.

CO-15 FORCE MAJEURE

CO-15.1 Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Agreement to the extent that such delay or failure is a result of Force Majeure.

CO-15.2 Notwithstanding Clause CO-15.1, each Party shall use all reasonable endeavours to continue to perform its obligations under the Call-Off Agreement for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under this Call-Off Agreement for a period in excess of one hundred and twenty (120) calendar days, either Party may terminate this Call-Off Agreement with immediate effect by notice in writing to the other Party.

CO-16 TRANSFER AND SUB-CONTRACTING

CO-16.1 The Supplier shall not assign, novate, sub-contract or in any other way dispose of this Call-Off Agreement or any part of it without the Customer's prior written approval which shall not be unreasonably withheld or delayed. Sub-Contracting any part of this Call-Off Agreement shall not relieve the Supplier of any obligation or duty attributable to the Supplier under this Call-Off Agreement.

CO-16.2 The Supplier shall be responsible for the acts and omissions of its Sub-Contractors as though they are its own.

CO-16.3 The Customer may assign, novate or otherwise dispose of its rights and obligations under the Call-Off Agreement or any part thereof to:

CO-16.3.1 any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Customer; or

CO-16.3.2 any private sector body which substantially performs the functions of the Customer

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier's obligations under the Call-Off Agreement.

CO-17 THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

CO-17.1 A person who is not party to this Call-Off Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Call-Off Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

CO-18 LAW & JURISDICTION

CO-18.1 This Call-Off Agreement and/or any non-contractual obligations or matters arising out of or in connection with it, shall be governed by and construed in accordance with the Laws of England and Wales and without prejudice to the dispute resolution procedures set out in Clause FW-14 or CO-22 (Dispute Resolution) each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

CO-19 ADDITIONAL G-CLOUD SERVICES

CO-19.1 The Customer may require the Supplier to provide the Additional G-Cloud Services. The Supplier acknowledges that the Customer is not obliged to take any Additional G-Cloud Services from the

Supplier and that there is nothing preventing the Customer from receiving services that are the same as or similar to the Additional G-Cloud Services from any third party.

CO-19.2 The Supplier shall provide Additional G-Cloud Services in accordance with any relevant Implementation Plan(s) and the Supplier shall monitor the performance of such Additional G-Cloud Services against the Implementation Plan(s).

CO-20 NOT USED

CO-21 VARIATION PROCEDURE

CO-21.1 The Customer may request in writing a variation to this Call-Off Agreement provided that such variation does not amount to a material change of the Framework Agreement and/or this Call-Off Agreement and is within the meaning of the Regulations and the Law. Such a change once implemented is hereinafter called a **"Variation**".

CO-21.2 The Supplier shall notify the Customer immediately in writing of any changes proposed or in contemplation in relation to G-Cloud Services or their delivery by submitting Variation request. For the avoidance of doubt such changes would include any changes within the Supplier's supply chain.

CO-21.3 In the event that:

(a) Either Party is unable to agree (agreement shall not be unreasonably withheld or delayed) to or provide the Variation;

(b) the Customer may:

(i) agree to continue to perform its obligations under this Call-Off Agreement without the Variation; or

(ii) terminate this Call-Off Agreement by giving thirty (30) written days notice to the Supplier.

CO-22 DISPUTE RESOLUTION

CO-22.1 The Customer and the Supplier shall attempt in good faith to negotiate a settlement of any dispute between them arising out of or in connection with this Call-Off Agreement within twenty (20) Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the Customer Representative and the Supplier Representative.

CO-22.2 If the dispute cannot be resolved by the Parties pursuant to this Clause, the Parties shall refer it to mediation unless the Customer considers that the dispute is not suitable for resolution by mediation.

CO-22.3 If the dispute cannot be resolved by mediation the Parties may refer it to arbitration.

CO-22.4 The obligations of the Parties under this Call-Off Agreement shall not be suspended, cease or be delayed by the reference of a dispute to mediation or arbitration pursuant to this Clause and the Supplier and Supplier's Staff shall continue to comply fully with the requirements of this Call-Off Agreement at all times.

Section 3 – DfE Special Terms

S3-1. Interpretations

S3-1.1 In this Contract the following words shall mean:

"Background IPR"	has the same meaning given to the term as in the Supplier's Terms in section 4 of this Contract;
"BPSS"	means the Government's Baseline Personal Security Standard, as contained in requirement 23 of the SPF;
"CESG"	is the UK government's National Technical Authority for Information Assurance. The website is http://www.cesg.gov.uk/Pages/homepage.aspx
"Charges"	the charges for the provision of the Services set out in and derived in accordance with S3-28, including any Milestone Payment, Stage Payment or Service Charge;
"Controlled Activity"	In relation to children as defined in Section 21 of the Safeguarding Vulnerable Groups Act 2006.
"Copyright"	means any and all copyright, design right (as defined by the Act) and all other rights of a like nature which may, during the course of this Contract, come into existence in or in relation to any Work (or any part thereof);
"Crown and/or Her Majesty"	Queen Elizabeth II and any successor to Her Majesty;
"Data", "Data Controller", "Data Processor", "Personal Data", "Sensitive Personal Data", "Data Subject", "Process" and "Processing"	shall have the meanings given to those terms by the Data Protection Act 1998
"Default"	any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub contractors in connection with or in relation to the subject-matter of this Agreement and in respect of which such party is liable to the other;
"Delay"	the period of time by which the implementation of the Services by reference to the Implementation Plan is delayed arising from a failure to Achieve a Milestone;
"Deliverable"	anything delivered or to be delivered under this Contract including the databases, and any reports, manuals and other documentation;
"Delivery"	time is of the essence in the delivery of any key milestone set out in any Implementation Plan.
"Departmental Assets"	includes but is not limited to DfE's premises, IT systems and information with a classification up to confidential.
"Deposited Software"	the Software the Source Code of which is to be placed in

	escrow;
"DfE's Data"	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Department; 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 Security Requirements"	means the security requirements of DfE set out in S3-4;
"Departmental Security Standards"	means the Department's specification for security that the Supplier is required to deliver.
"DSU"	Departmental Security Unit
"Escrow Agent"	the agent appointed by the Customer and/or the Supplier to hold the Deposited Software;
"Escrow Agreement"	the agreement entered into between the Customer, the Supplier and the Escrow Agent, pursuant to the Escrow Terms;
"Force Majeure Event"	any cause affecting the performance by a party of its obligations arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or Regulatory Bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Supplier, the Supplier Personnel or any other failure in the Supplier or the Sub-contractor's supply chain;
"Forensic Readiness Policy"	means a policy that is supported by a contract with a suitably qualified third party to provide capability to forensically investigate incidents, or a policy that will allow DfE to directly access and forensically examine ICT systems including hardware;
"Good Industry 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"	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.
"Her Majesty's Government"	the duly elected Government for the time being during the reign of Her Majesty and/or any department, committee, office, servant or officer of such Government;
"HMG IA Standard"	means the Government's Information Assurance Standard(s);
"HMSO"	Her Majesty's Stationery Office;
"ICT Environment"	the DfE's system and the Supplier system;
"ICT"	information and communications technology;
"Information Assurance"	means information controls and standards;
"Insolvency Event"	the occurrence of any of the following events (or any event analogous to any of the following in a jurisdiction other than England and Wales) in relation to the relevant entity: (a) the entity passing a resolution for its winding up or a court of competent jurisdiction making an order for the entity to be wound up or dissolved or the entity being otherwise dissolved; (b) the appointment of an administrator of, or the making of an administration order in relation to, the entity or the appointment of a receiver or administrative receiver of, or an encumbrancer taking possession of or selling, the whole or part of the entity's undertaking, assets, rights or revenue; (c) the entity entering into an arrangement, compromise or composition in satisfaction of its debts with its creditors or any class of them or taking steps to obtain a moratorium or making an application to a court of competent jurisdiction for protection from its creditors; (d) the entity being unable to pay its debts or being deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or (e) the entity entering into any arrangement, compromise or composition in satisfaction of its debts with its creditors; However, a resolution by the relevant entity or a court order that such entity be wound up for the purpose of a bona fide reconstruction or amalgamation shall not amount to an Insolvency Event; amalgamation shall not amount to an Insolvency Event;
"Intellectual Property Rights"	patents, trademarks, service marks, design rights (whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom) other than the Background

	IPR.
“IT Security Health Check”	means an assessment to identify vulnerabilities in IT systems and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
"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;
“Operational Requirement”	means a report on the operational requirement of the NCT programme which justifies the implementation of a security measure;
"Personal Data"	shall have the same meaning as set out in the Data Protection Act 1998;
“Personnel Security Clearance”	means a process and standards put in place to assure trustworthiness, integrity and reliability of all Personnel, including as a minimum requirement that all staff are subject to BPSS recruitment controls;
“Personnel Security Standard”	A government wide requirement including checks on identity, employment history, nationality and immigration status and the declaration of unspent criminal records.
“Government Security Classification Policy ”	means the system of grading and applying the Classification criteria;
“Classification’”	means the marking of Classified Assets according to the Government Security Classification Policy;
“Protective Security”	means the level of security provided by meeting the SPF mandatory requirements;
“Classified Assets”	means all data, assets, equipment and other materials classified OFFICIAL or above as described in the Government Security Classification Policy.
“Classified Data”	means Classified Assets in the form of data;
“Public Records Act”	means the Public Records Act 1958 as amended, inter alia, by the Public Records Act 1967 and FOIA;
“Regulated Activity”	In relation to children as defined in Part 1 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006.
“Regulated Activity” Provider	As defined in Section 6 of the Safeguarding Vulnerable

	Groups Act 2006.
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Agreement or any other affairs of the Authority and "Regulatory Body" shall be construed accordingly;
"Required Action"	has the meaning given in clause S3-12 (Step-In Rights);
“DSAM”	means the DSU Security Assurance Model required by DfE to support security assurance activities produced in accordance with the DSAM published by DfE;
"Security Plan"	the Supplier's security plan prepared as part of their tender and included as a schedule (Security Requirements) to the Contract;
"Security Policy"	the DfE's security policy annexed to the Security Requirements and Plan schedule as updated from time to time;
"Software"	Specially Written Software, Supplier Software and Third Party Software;
"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 technical information and documentation necessary for the use, reproduction, modification and enhancement of such software;
"Specially Written Software"	any software written by or on behalf of the Supplier for the DfE and supplied to the DfE.
“SPF”	means the Government’s Security Policy Framework.
"Staff Vetting Procedures"	the DfE's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;
"the Act"	means the Copyright Designs and Patents Act 1988;
"Supplier Personnel"	all employees, agents, consultants and Suppliers of the Supplier and/or of any Sub-contractor;
"Supplier Software"	software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services;
“Work”	any and all Works including but not limited to literary, dramatic, musical or artistic works, sound recordings, films,

	broadcasts or cable programmes, typographical arrangements and designs (as the same are defined in the Copyright Designs and Patents Act 1988) which are created from time to time during the course of this Contract by the Supplier or by or together with others at the Supplier's request or on its behalf and where such works directly relate to or are created in respect of the performance of this Contract or any part of it but does not include the Background IPR.
"Working Day"	any day other than a Saturday, Sunday or public holiday in England and Wales.

S3-2. Intellectual Property Rights and Copyright

S3-2.1 The Supplier agrees that the Crown shall be legally and beneficially entitled to any and all Intellectual Property Rights and Copyright created by the Supplier in the performance of this Contract (including the Deliverables and Specially Written Software) and the Supplier hereby assigns to the Crown any and all residual title which it may have in any and all such Intellectual Property Rights and/or Copyright.

S3-2.2 The Supplier undertakes that it shall, from time to time, take all such steps and execute all such documents as the Crown or HMSO on its behalf may reasonably require to fully vest in the Crown any and all residual title, whether legal or beneficial, to the Intellectual Property Rights and/or Copyright.

S3-2.3 The Supplier grants to the Crown or HMSO a royalty free, perpetual, non-exclusive, sub-licensable licence to use any Background IPR, including any Background IPR that is embedded in the Supplier Software and/or Deliverables, solely in connection with the use of the Supplier Software and/or Deliverables. The aforementioned licence shall survive termination of this Contract.

S3-3. COPYRIGHT WARRANTIES

S3-3.1 The Supplier now warrants to the Crown, HMSO and the Department (and to any assignees and licensees of each) that all Works will not infringe in whole or in part any copyright or like right or any other intellectual property right of any other person (wheresoever) and agrees to indemnify and hold harmless Her Majesty and/or Her Majesty's Government against any and all claims, demands, proceedings, expenses and losses, including any of a consequential nature, arising directly or indirectly out of any act of the foregoing in relation to any Work, where such act is or is alleged to be an infringement of a third party's copyright or like right or other intellectual property right (wheresoever).

S3-3.2 The warranty and indemnity contained in Clause S3-3.1 above shall survive the termination of this Contract and shall exist for the life of the Copyright.

S3-4. Departmental Security Standards

S3-4.1 The Supplier will assure the Department that they can comply with its Departmental Security Standards for Suppliers which include but are not constrained to the following paragraphs

S3-4.2 Where the Supplier will process personal data on behalf of the Department or other data deemed sensitive by the Department or supply ICT products or services to, or on behalf of, the Department, the Supplier will be expected to have achieved, and be able to maintain, certification to the appropriate level, under the HMG Cyber Essentials Scheme or equivalent. The certification must have a scope relevant to the services supplied to, or on behalf of, the Department. Alternatively, the Supplier must demonstrate, to the satisfaction of the Department, compliance with the requirements of the Cyber Essentials Scheme.

S3-4.3 The Supplier will be expected to have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Requirements Specification). The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department and the statement of applicability must be acceptable to the Department, including the application of an appropriate selection of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

S3-4.4 The Supplier will adopt the UK Government Security Classification Policy in respect of any Departmental Data being handled in the course of providing this service, and will handle this 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).

S3-4.5 The Supplier will have in place and maintain physical (e.g. door access) and logical (e.g. identification and authentication) access controls to ensure only authorised access to Departmental Data.

S3-4.6 The Supplier will have in place and maintain technical safeguards to protect Departmental Data, including but not limited to: Good Industry Standard anti-virus and firewalls; up-to-date patches for operating system, network device, and application software.

S3-4.7 Any electronic transfer methods across public space or cyberspace must be protected via encryption which has been certified to FIPS140-2 or certified under a CESG (e.g. CAPS or CPA) or CESG-endorsed scheme, and the method shall be approved by the Department prior to being used for the transfer of any Departmental Data.

S3-4.8 Paper documents containing Departmental Data shall be transmitted, both within and outside company premises in such a way as to make sure that no unauthorised person has access.

S3-4.9 Any portable removable media (including but not constrained to pen drives, memory sticks, CDs, DVDs, PDPs, USB devices) which handle, store or process in any way Departmental Data to deliver and support the service, shall be under the configuration management of the (sub-)contractors providing the service, shall be necessary to deliver the service, and shall be full-disk encrypted using a product which has been certified to FIPS140-2 or certified under a CESG (e.g. CAPS or CPA) or CESG-endorsed scheme or uses another encryption standard that is acceptable to the Department.

S3-4.10 All portable ICT devices (including but not limited to laptops, PDAs, smartphones) which handle, store or process in any way Departmental Data to deliver and support the service, shall be under the configuration management of the (sub-)contractors providing the service and shall be full-disk encrypted using a product which has been certified to FIPS140-2 or been certified under a CESG (e.g. CAPS or CPA) or CESG-endorsed scheme or uses another encryption standard that is acceptable to the Department.

S3-4.11 Storage of Departmental Data on any portable devices or media shall be limited to the minimum required to deliver the business requirement.

S3-4.12 Access by Supplier staff to Departmental Data shall be confined to those individuals who have a “need-to-know” and whose access is essential for the purpose of their duties. All employees with direct or indirect access to Departmental Data must be subject to pre-employment checks equivalent to or higher than the Baseline Personnel Security Standard (BPSS): Details of the standard are available at the HMG website https://www.gov.uk/government/publications/security-policy-framework

S3-4.13 All Supplier employees who handle Departmental Data must have annual awareness training in protecting information.

S3-4.14 The Supplier will deliver services that are compliant with HMG Security Policy Framework in conjunction with CESG Information Assurance Policy Portfolio. The Supplier will provide the DfE with evidence of compliance for the services to be delivered, including, but not limited to:

- DSU Security Assurance Model (DSAM)
- Full Risk Assessments for the Services, including Residual Risk Statements
- Security Operating Procedures (SyOPs) for all user types
- Forensic Readiness Policy

S3-4.15 The Supplier will provide details of:

- Any existing HMG accreditations including the body awarding accreditation; the scope of the accreditation; any caveats; date awarded and duration; residual risk statement. Evidence of accreditation will be required.
- Progress in achieving HMG accreditation including whether documentation has been produced and submitted. If HMG accreditation is in progress, the Supplier will state who the awarding organisation will be and date expected.

S3-4.16 If no current HMG accreditation is held the Supplier will undergo appropriate assurance as determined by the Department which may involve HMG accreditation by DfE Accreditor. In this case the Supplier will support the production of the necessary documentation (e.g. DSAM). This will include obtaining the necessary professional security expertise.

S3-4.17 The Supplier will provide details of the most recent IT Health Check conducted and submit the report to the Department. If no IT Health Check has been carried out in the last year, or, if it has not been performed by a CHECK provider then the Supplier will be required to arrange for a CHECK IT Health Check; the scoping to be agreed with the Department. In the event of significant issues being identified, a follow up remediation test will be required.

S3-4.18 An IT Health Check to be performed by a CHECK provider will further be required annually for the duration of the contract. The results of which must be shared with the Department.

S3-4.19 The Supplier will provide details of any proposal to store or host Departmental Data outside the UK or to perform ICT management or support from outside the UK and will not go ahead with such a proposal without prior agreement from the Department.

S3-4.20 Departmental Data being handled in the course of providing this service must be segregated from other data on the Supplier's own IT equipment to protect the Departmental Data and enable it to be securely deleted when required. In the event that it is not possible to segregate the Departmental Data then the Supplier is required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause S3-4.21.

S3-4.21 At the end of the contract or in the event of failure or obsoletion, all equipment holding Departmental Data must be securely cleansed or destroyed using a CESG approved product or method and in accordance with HMG standards. Where this is not possible e.g. for legal or regulatory reasons, or technical reasons such as where there is storage area network (SAN) or shared backup tapes, then the Supplier must protect the equipment until the time (which may be long after the end of the contract) when it can be securely cleansed or destroyed.

S3-4.22 All paper holding Departmental Data must be securely protected whilst in the Supplier's care and securely destroyed when no longer required in accordance with HMG standards.

S3-4.23 The Supplier must have ISO 22301 conformant Business Continuity plans and processes including IT disaster recovery plans and procedures to ensure that the delivery of the contract is not adversely affected in the event of an incident or crisis. The Supplier must describe how this requirement will be met.

S3-4.24 Any non-compliance with these Departmental Security Standards for Suppliers, or any suspected or actual breach of the confidentiality or integrity of Departmental Data being handled in the course of providing this service, shall be immediately escalated to the Department by a method agreed by both parties.

S3-4.25 The Supplier shall contractually enforce all these Departmental Security Standards for Suppliers onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

S3-4.26 The Department reserves the right to audit the Supplier or sub-contractors providing the service within a mutually agreed period, but always within seven days of notice to audit being given, in respect to the Supplier's or sub-contractors compliance with the clauses contained in this Section.

S3-5. Ownership of Rights in the Deliverables and the Specially Written Software

S3-5.1 Title to and risk in any tangible property embodying all Deliverables and Specially Written Software shall vest in the Department upon acceptance.

S3-5.2 The Supplier hereby grants, or shall procure that the owner of the Background IPR in the Deliverables and/or the Specially Written Software grants, to the Department, a non-exclusive licence to use, reproduce, modify, adapt and enhance the Deliverables and the Specially Written Software. Such licence shall be perpetual and irrevocable.

S3-5.3 The Supplier shall supply the Department with a copy of the source code of any Specially Written Software.

S3-5.4 The Department shall be entitled to engage a third party to use, reproduce, modify and enhance the Deliverables and the Specially Written Software on behalf of the Department provided that such third party shall have entered into a confidentiality undertaking with the Department.

S3-6. Supplier's co-operation with Departmental objectives

S3-6.1 In performing the Contract, the Supplier shall at all times co-operate with the Department to maximise value for money, sustainable delivery where it is not detrimental to the interests of either Party to do so.

S3-7. Sustainable Considerations

S3-7.1 The Supplier shall in all his operations, including purchase of materials goods and services, adopt a sound proactive sustainable approach, designed to minimise harm to the environment, society and economy and be able to provide proof of doing so to the Contract Manager on demand.

S3-7.2 The Supplier shall ensure that any personnel provided under this Contract including those of any sub-contractors, who have unsupervised access to Departmental Assets meet the Personnel Security Standards and shall provide evidence that the checks have been performed on request.

S3-7.3 A breach of this Clause S-7 shall entitle the Department to terminate the contract immediately.

S3-8. Equality

S3-8.1 The Supplier shall at all times provide the service in accordance with the Department's commitment to

equal opportunities to all sections of the community including the obligations placed on public bodies by the Equalities Act 2006, the Disability Discrimination Act 2005, the Employment Equality (Age) Regulations, the Race Relations Amendment Act 2000 and the Sex Discrimination Act 1975.

S3-8.2 The Supplier shall establish adequate managerial and supervisory arrangements for staff to be made aware of and to comply with discrimination legislation and the equality specifications within this contract.

S3-8.3 The Supplier shall ensure that sufficient, instructed and competent staff are available to provide services to all sections of the community including those who do not speak English.

S3-8.4 The Supplier shall support and co-operate with Department initiatives aimed at improving services (and/or access to services) to different groups in the community

S3-8.5 The Supplier shall provide any information regarding the delivery of its services to ensure the Department meets its statutory obligations.

S3-9. Staffing Security

S3-9.1 The Supplier shall comply with the Staff Vetting Procedures in respect of all Supplier Personnel employed or engaged in the provision of the Services. The Supplier confirms that all Supplier Personnel employed or engaged by the Supplier to work on this Contract were vetted and recruited on a basis that is equivalent to and no less strict than the Staff Vetting Procedures.

S3-10. Security Requirements

S3-10.1 The Supplier shall comply, and shall procure the compliance of the Supplier Personnel, with the Security Plan.

S3-10.2 The Department shall notify the Supplier of any changes or proposed changes to the Security Plan.

S3-10.3 If the Supplier believes that a change or proposed change to the Security Plan will have a material and unavoidable cost implication to the Services it may submit a business case for any additional costs. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs.

S3-10.4 Until and/or unless a change to the charges is agreed by the Department pursuant to clause S3-10.3 the Supplier shall continue to perform the Services in accordance with its existing obligations.

Malicious Software

S3-10.5 The Supplier shall, as an enduring obligation throughout the period of the Contract, use the latest versions of anti-virus definitions available to check for and delete Malicious Software from the ICT Environment.

S3-10.6 Notwithstanding clause S3-10.5, 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 Department's Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

S3-10.7 Any cost arising out of the actions of the parties taken in compliance with the provisions of clause S3-10.6 shall be borne by the parties as follows:

S3-10.7.1 by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software or the Department's Data (whilst the Department's Data was under the control of the Supplier); and

S3-10.7.2 by the Department if the Malicious Software originates from the Department's Software or the Department's Data (whilst the Department's Data was under the control of the Department).

S3-11. Termination

S3-11.1 In addition to the provisions of clause CO-9, the Customer may terminate this Call-off Agreement with immediate effect by notice in writing where the Supplier:

S3-11.1.1 is convicted (or being a company, any officers or representatives of the Supplier are convicted) of a criminal offence related to the business or professional conduct

S3-11.1.2 (or being a company, any officers or representatives of the Supplier) by a deliberate and unreasonable act destroys the Customer Personal Data at any time during the term of this Call-Off Agreement, unless the Customer has given its written instruction or consent to do so (such consent not to be unreasonably withheld or delayed);

S3-11.1.3 fails (or being a company, any officers or representatives of the Supplier fail) to fulfil his/their obligations relating to the payment of Social Security contributions;

S3-11.1.4 fails (or being a company, any officers or representatives of the Supplier fail) to fulfil his/their obligations relating to payment of taxes;

S3-11.1.5 fails (or being a company, any officers or representatives of the Supplier fail) to disclose any serious misrepresentation in supplying information required by the Department in or pursuant to this Call-Off Agreement.

S3-12. Step In Rights

S3-12.1 The Department may take action under this clause in the following circumstances:

S3-12.1.1 there is a Default entitling the Department to terminate in accordance with Clause CO-9 and S3-11;

S3-12.1.2 there is a Default by the Supplier that is materially preventing or materially delaying the performance of the Services or Project or any part of the Services or Project;

S3-12.1.3 there is a Delay that has or the Department reasonably anticipates will result in the Supplier's failure to achieve a milestone;

S3-12.1.4 a Force Majeure Event occurs which materially prevents or materially delays the performance of the Services or Project or any part of the Services or Project;

S3-12.1.5 where the Supplier is not in breach of its obligations under this Contract but the Department considers that the circumstances constitute an emergency;

S3-12.1.6 where a Regulatory Body has advised the Department that the exercise by the Department of its rights under this clause is necessary;

S3-12.1.7 because a serious risk exists to the health or safety of persons, property or the environment;

S3-12.1.8 to discharge a statutory duty; and/or on the occurrence of an Insolvency Event in respect of the Supplier.

Action To Be Taken Prior To Exercise Of The Right Of Step-in

S3-12.2 Before the Department exercises its right of step-in under this Clause S3-12 it shall permit the Supplier the opportunity to demonstrate to the Department's reasonable satisfaction within 5 Working Days that the Supplier is still able to provide the Services or Project in accordance with the terms of this Contract and/or remedy the circumstances giving rise to the right to step-in without the requirement for the Department to take action.

S3-12.3 If the Department is not satisfied with the Supplier's demonstration pursuant to clause S3-12.2, the Department may:

S3-12.3.1 where the Department considers it expedient to do so, require the Supplier by notice in writing to take those steps that the Department considers necessary or expedient to mitigate or rectify the state of affairs giving rising to the Department's right to step-in;

S3-12.3.2 appoint any person to work with the Supplier in performing all or a part of the Services or Project (including those provided by any Sub-contractor); or

S3-12.3.3 take the steps that the Department considers appropriate to ensure the performance of all or part of the Services or Project (including those provided by any Sub-contractor).

S3-12.4 The Supplier shall co-operate fully and in good faith with the Department, or any other person appointed in respect of clause S3-12.3.2, and shall adopt any reasonable methodology in providing the Services or Project recommended by the Department or that person.

Exercise of the Right of Step-in

S3-12.5 If the Supplier:

S3-12.5.1 fails to confirm within 10 Working Days of a notice served pursuant to clause S3-12.3.1 that it is willing to comply with that notice; or

S3-12.5.2 fails to work with a person appointed in accordance with clause S3-12.3.1; or

S3-12.5.3 fails to take the steps notified to it by the Department pursuant to clause S3-12.3.1,

then the Department may take action under this clause either through itself or with the assistance of third party Suppliers, provided that the Supplier may require any third parties to comply with any confidentiality undertaking

S3-12.6 If the Department takes action pursuant to clause S3-12.5, the Department shall serve notice ("Step-in Notice") on the Supplier. The Step-in Notice shall set out the following:

S3-12.6.1 the action the Department wishes to take and in particular the Services it wishes to control;

S3-12.6.2 the reason for and the objective of taking the action and whether the Department reasonably believes that the primary cause of the action is due to the Supplier's Default;

S3-12.6.3 the date it wishes to commence the action;

S3-12.6.4 the time period which it believes will be necessary for the action;

S3-12.6.5 whether the Department will require access to the Supplier's premises;

S3-12.6.6 to the extent practicable, the effect on the Supplier and its obligations to provide the Services during the period the action is being taken.

S3-12.7 Following service of a Step-in Notice, the Department shall:

S3-12.7.1 take the action set out in the Step-in Notice and any consequential additional action as it reasonably believes is necessary to achieve (together, the "Required Action");

S3-12.7.2 keep records of the Required Action taken and provide information about the Required Action to the Supplier;

S3-12.7.3 co-operate wherever reasonable with the Supplier in order to enable the Supplier to continue to provide any Services in relation to which the Department is not assuming control; and

S3-12.7.4 act reasonably in mitigating the cost that the Supplier will incur as a result of the exercise of the Department's rights under this clause.

S3-12.8 For so long as and to the extent that the Required Action is continuing, then:

S3-12.8.1 the Supplier shall not be obliged to provide the Services or Project to the extent that they are the subject of the Required Action;

S3-12.8.2 subject to clause S3-12.9, the Department shall pay to the Supplier the Charges after the deduction of any applicable Service Credits, Delay Payments and the Department's costs of taking the Required Action.

S3-12.9 If the Required Action results in:

S3-12.9.1 the degradation of any Services or Project not subject to the Required Action; or

S3-12.9.2 the non-achievement of a milestone,

beyond that which would have been the case had the Department not taken the Required Action, then the Supplier shall be entitled to an agreed adjustment of the Charges, provided that the Supplier can demonstrate to the reasonable satisfaction of the Department that the Required Action has led to the degradation or non-achievement.

S3-12.10 Before ceasing to exercise its step in rights under this clause the Department shall deliver a written notice to the Supplier ("Step-Out Notice"), specifying:

S3-12.10.1 the Required Action it has actually taken; and

S3-12.10.2 the date on which the Department plans to end the Required Action ("Step-Out Date") subject to the Department being satisfied with the Supplier's ability to resume the provision of the Services or Project and the Supplier's plan developed in accordance with clause S3-12.11.

S3-12.11 The Supplier shall, following receipt of a Step-Out Notice and not less than 20 Working Days prior to the Step-Out Date, develop for the Department's approval a draft plan ("Step-Out Plan") relating to the resumption by the Supplier of the Services or Project, including any action the Supplier proposes to take to ensure that the affected Services or Project satisfy the requirements of this Contract.

S3-12.12 If the Department does not approve the draft Step-Out Plan, the Department shall inform the Supplier of its reasons for not approving it. The Supplier shall then revise the draft Step-Out Plan taking those reasons into account and shall re-submit the revised plan to the Department for the Department's approval. The Department shall not withhold or delay its approval of the draft Step-Out Plan unnecessarily.

S3-12.13 The Supplier shall bear its own costs in connection with any step-in by the Department under this Clause S3-11, provided that the Department shall reimburse the Supplier's reasonable additional expenses incurred directly as a result of any step-in action taken by the Department under:

S3-12.13.1 clauses S3-12.1.4 or S3-12.1.7; or

S3-12.13.2 clauses S3-12.1.8, S3-12.1.9 and S3-12.1.10 (insofar as the primary cause of the Department serving the Step-In Notice is identified as not being the result of a Supplier's Default).]

S3-13. Tax Indemnity

S3-13.1 Where the Consultant is liable to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration.

S3-13.2 Where the Consultant is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration.

S3-13.3 The Department may, at any time during the term of this contract, ask the Consultant to provide information which demonstrates how the Consultant complies with Clauses S3-13.1 and S3-13.2 above or why those Clauses do not apply to it.

S3-13.4 A request under Clause S3-13.3 above may specify the information which the Consultant must provide and the period within which that information must be provided.

S3-13.5 The Department may terminate this contract if-

(a) in the case of a request mentioned in Clause S3-13.3 above if the Consultant:

(i) fails to provide information in response to the request within a reasonable time, or

(ii) provides information which is inadequate to demonstrate either how the Consultant complies with Clauses S3-13.1 and S3-13.2 above or why those Clauses do not apply to it;

(b) in the case of a request mentioned in Clause S3-13.4 above, the Consultant fails to provide the specified information within the specified period, or

(c) it receives information which demonstrates that, at any time when Clauses S3-13.1 and S3-13.2 apply, the Consultant is not complying with those Clauses.

S3-13.6 The Department may supply any information which it receives under Clause S3-13.3 to the Commissioners of Her Majesty's Revenue and Customs for the purpose of the collection and management of revenue for which they are responsible.

S3-13.7 The Consultant warrants and represents to the Department that it is an independent Supplier and, as such, bears sole responsibility for the payment of tax and national insurance contributions which may be found due from it in relation to any payments or arrangements made under this Contract or in relation to any payments made by the Consultant to its officers or employees in connection with this Contract.

S3-13.8 The Consultant will account to the appropriate authorities for any income tax, national insurance, VAT and all other taxes, liabilities, charges and duties relating to any payments made to the Consultant under this Contract or in relation to any payments made by the Consultant to its officers or employees in connection

with this Contract.

S3-13.9 The Consultant shall indemnify Department against any liability, assessment or claim made by the HM Revenue and Customs or any other relevant authority arising out of the performance by the parties of their obligations under this Contract (other than in respect of employer's secondary national insurance contributions) and any costs, expenses, penalty fine or interest incurred or payable by Department in connection with any such assessment or claim.

S3-13.10 The Consultant authorises the Department to provide the HM Revenue and Customs and all other departments or agencies of the Government with any information which they may request as to fees and/or expenses paid or due to be paid under this Contract whether or not Department is obliged as a matter of law to comply with such request.

S3-14. TUPE

S3-14.1 The Parties recognise that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE) may apply in respect of the award of the Contract, and that for the purposes of those Regulations, the undertaking concerned (or any relevant part of the undertaking) shall transfer to the Supplier on the commencement of the Contract.

S3-14.2 During the period of six months preceding the expiry of the Contract or after the Department has given notice to terminate the Contract or the Supplier stops trading, and within 20 working days of being so requested by the Department, the Supplier shall fully and accurately disclose to the Department for the purposes of TUPE all information relating to its employees engaged in providing Services under the Contract, in particular, but not necessarily restricted to, the following:

S3-14.2.1 the total number of staff whose employment with the Supplier is liable to be terminated at the expiry of this Contract but for any operation of law; and

S3-14.2.2 for each person, age and gender, details of their salary, and pay settlements covering that person which relate to future dates but which have already been agreed and their redundancy entitlements (the names of individual members of employed staff do not have to be given); and

S3-14.2.3 full information about the other terms and conditions on which the affected staff are employed (including but not limited to their working arrangements), or about where that information can be found; and

S3-14.2.4 details of pensions entitlements, if any; and

S3-14.2.5 job titles of the members of staff affected and the qualifications required for each position.

S3-14.3 The Supplier shall permit the Department to use the information for the purposes of TUPE and of re-tendering. The Supplier will co-operate with the re-tendering of the Contract by allowing the Transferee to communicate with and meet the affected employees and/or their representatives.

S3-14.4 The Supplier agrees to indemnify the Department fully and to hold it harmless at all times from and against all actions, proceedings, claims, expenses, awards, costs and all other liabilities whatsoever in any way connected with or arising from or relating to the provision of information under Clause S3-14.2.

S3-14.5 Not Used.

S3-14.6 In the event that the information provided by the Supplier in accordance with Clause S3-14.2 above becomes inaccurate, whether due to changes to the employment and personnel details of the affected employees made subsequent to the original provision of such information or by reason of the Supplier becoming aware that the information originally given was inaccurate, the Supplier shall notify the Department of the inaccuracies and provide the amended information.

S3-14.7 The provisions of this Condition shall apply during the continuance of this Contract and indefinitely after its termination.

S3-15. Safeguarding children and vulnerable adults

S3-15.1 The Supplier will put in place safeguards to protect children and vulnerable adults from a risk of significant harm which could arise from the performance of this Contract. The Supplier will agree these safeguards with the Department before commencing work on the Contract.

S3-15.2 In addition, the Supplier will carry out checks with the Disclosure and Barring Service (DBS checks) on all staff employed on the Contract in a Regulated Activity. Suppliers must have a DBS check done every three

years for each relevant member of staff for as long as this Contract applies. The DBS check must be completed before any of the Supplier's employees work with children in Regulated Activity.

S3-15.3 The Supplier shall immediately notify the Department of any information that it reasonably requests to enable it to be satisfied that the obligations of this Clause S3-15 have been met.

S3-15.4 The Supplier shall not employ or use the services of any person who is barred from, or whose previous conduct or records indicate that he or she would not be suitable to carry out Regulated Activity or who may otherwise present a risk to children or vulnerable adults.

S3-16. ESCROW

S3-16.1 The Supplier shall ensure that the Source Code of all Software supplied to the Customer shall be deposited in escrow with an agreed Escrow Agent on the basis of the appropriate standard agreement or on such other terms as the Customer, the Supplier and the Escrow Agent shall agree.

S3-17. Failures

S3-17.1 The Supplier shall promptly warn DfE whenever the Supplier has reasonable grounds to believe that any development (including failure on the part of the Supplier to carry out its obligations and responsibilities under this Agreement) will have, or threatens to have, a detrimental effect on the Services. At DfE's request, the Supplier shall take all reasonable steps to prevent such development from occurring and to prevent its reoccurrence, provided that where the relevant development has arisen as a direct result of DfE's breach of this Agreement, DfE will pay all of the Supplier's reasonable costs in taking such steps, such costs to be calculated on a Time And Materials Basis.

S3-17.2 If the Supplier fails to perform the Services in accordance with this Agreement (a "Defect") then, without prejudice to any other rights or remedies it may have under this Agreement or otherwise, DfE may require the Supplier by notice in writing, at the Supplier's own expense, to remedy any default or to re-perform any Service affected by the Defect within a reasonable time specified in the notice. If the Supplier fails to remedy a Defect within the time specified, DfE may, or may instruct a third party to, remedy that Defect, the reasonable costs of which shall be borne by the Supplier. Where: (i) DfE has withheld payment of the Charges for the Service affected by the Defect; or (ii) DfE has not yet paid the Charges for the Service affected by the Defect and is entitled to withhold payment of such Charges, such reasonable costs to be borne by the Supplier shall be comprised of only those costs that are over and above the amount of the Charges that DfE has so withheld or is entitled to withhold.

S3-17.3 If the Supplier fails to perform the Services in accordance with this Agreement, then without prejudice to any other rights or remedies it may have under this Agreement or otherwise, DfE may require the Supplier by notice in writing to carry out an investigation into the cause of such failure. The Supplier shall carry out such an investigation in accordance with Good Industry Practice, promptly and at its own cost and shall provide a complete and accurate report of that investigation to DfE.

S3-17.4 The obligations in this Clause S3-17 are without prejudice to any other obligations of the Supplier or rights of DfE whether under this Agreement or otherwise.

S3-18. Branding of the Website

Licence of Trade Marks

S3-18.1 DfE hereby grants the Supplier a non-exclusive royalty-free licence to use the Trade Marks during the Term in the Territory on or in relation to the Website or related materials solely as is reasonably necessary for the provision of the Services.

Quality and Control

S3-18.2 The Supplier shall ensure that the Website carries the Trade Marks that DfE requires (if any). The right to use the Trade Marks is conditional on the Supplier's compliance with the Brand Guidelines (as amended by DfE from time to time upon reasonable written notice to the Supplier). The Supplier shall not display any trade marks (other than the Trade Marks) or other promotional information on the Website or any other materials delivered or made available to schools or Local Authorities without DfE's prior written consent.

S3-19. Regulations

Compliance

S3-19.1 Save where DfE determines that a Regulatory Change is not required in accordance with Clause S3-19.5 – S3-19.7 (and then only to the extent of that Regulatory Change), the Supplier shall comply, and shall ensure that its Subcontractors and Personnel comply, with all Regulations and Government standards (in-

cluding the e-government interoperability framework) at all times when performing the Services, insofar as such Regulations and Government standards apply to the Services.

S3-19.2 The Supplier shall ensure that the Services are performed so that DfE complies with all Regulations, to the extent that DfE's compliance with the Regulations is dependent on the Services.

S3-19.3 Each of the Parties shall advise the other immediately if it becomes aware of any non-compliance or suspected non-compliance by the Supplier with the provisions of Clause S3-19.1 or S3-19.2 in connection with the performance of the Services. If such an event occurs, the Supplier shall promptly make available to DfE any information that DfE reasonably requires for the purposes of any further investigation of such non-compliance or suspected non-compliance.

Correspondence

S3-19.4 If the Supplier receives any correspondence from any Regulatory Authority (save to the extent in respect of: (i) corporation tax; or (ii) national insurance for employees of the Supplier) that relates to the Services, it shall promptly provide a copy of that correspondence to DfE unless it is prevented from doing so by the Regulations or a Regulatory Authority. The Supplier shall give DfE a reasonable opportunity to discuss and make representations on the practical and written response to such correspondence, and shall only respond to the Regulatory Authority if:

S3-19.4.1 the terms of the response have been approved by DfE (such approval not to be unreasonably withheld or delayed); or

S3-19.4.2 the Supplier is required by Regulations to respond to the Regulatory Authority without DfE's consent.

Changes to Regulations

S3-19.5 If a change to any Regulation means a change to the Services or Charges is required (a "Regulatory Change"), the Supplier shall, subject to Clauses S3-19.6 and S3-19.7, make that Regulatory Change as soon as reasonably possible.

S3-19.6 The Parties shall seek to agree the details and cost of the Regulatory Change in accordance with the Change Control Procedure.

S3-19.7 If there is any disagreement between the Parties regarding any Regulatory Change or potential Regulatory Change:

S3-19.7.1 DfE shall have the right to determine: (a) whether a Regulatory Change is required; and (b) how the Supplier shall implement that Regulatory Change, in which case the Supplier shall promptly implement the Regulatory Change as determined by DfE in accordance with this Clause S3-19.7.1; and

S3-19.7.2 DfE shall pay to the Supplier the costs of implementing the Regulatory Change which shall be equivalent to the Supplier's reasonable costs, calculated on a Time and Materials Basis, save that if the Regulatory Change is carried out for other service recipients of the Supplier, DfE shall only bear an equitable proportion of the Supplier's reasonable costs.

S3-20. Security and Backup

S3-20.1 Without limiting any of its other obligations under this Agreement the Supplier shall, and shall ensure that its Subcontractors shall:

S3-20.1.1 comply with the DfE Security Requirements; and

S3-20.1.2 ensure that DfE Data is kept logically separate from the data of any of the Supplier's other service recipients.

S3-20.2 The Supplier shall not, and shall use reasonable endeavours in accordance with Good Industry Practice to ensure that its Subcontractors shall not, knowingly or intentionally introduce a Virus into the Application and shall take precautions in accordance with Good Industry Practice to prevent:

S3-20.2.1 any Virus from being introduced into the Application or the networks and websites of DfE, including ensuring that virus protection software is used and kept up to date;

S3-20.2.2 unauthorised access or use of the Application; or

S3-20.2.3 unauthorised disclosure, loss, destruction or alteration of any DfE Data.

S3-20.3 The Supplier shall promptly notify DfE should it become aware of, or reasonably suspect, the occurrence of any of the events referred to in Clause S3-20.2 and shall promptly take all steps necessary to remedy the event and prevent its reoccurrence.

S3-20.4 Prior to the Customer Acceptance Tests, the Supplier will provide to DfE a security document covering the requirements listed in the DfE Security Requirements to support the build and recovery documentation (the "Security Document"). The Supplier shall ensure that this Security Document includes:

S3-20.4.1 Operating system: a detailed outline of the operating system level security implemented by the Supplier, including group policies, lightweight directory access protocol configurations, domain and user accounts and related access permissions;

S3-20.4.2 Database: confirmation of the base security requirements that the Supplier adhered to for any database or data source used in connection with the Application, including in respect of connectivity, e.g. virtual private network connections for data transmission services/SQL server integration services packages. The Security Document provided by the Supplier shall detail any key administration credentials required for system build or recovery; and

S3-20.4.3 Application: a detailed account of security aspects specific to the system, including administrator or specific end-user credentials, secured socket layer (SSL) certificate details, domain/sub-domain configuration and any additional security layers.

S3-20.5 The Supplier shall continue to have in place and keep up-to-date the Security Document and shall provide the most recent version of such Security Document to DfE as soon as reasonably practicable on request from DfE from time to time.

S3-20.6 The Supplier shall co-operate with any security audit or investigation which is carried out by or on behalf of DfE, including providing access, information or material in its possession or control and implementing new security measures, to the extent reasonably requested by DfE provided that nothing in this clause S3-20.6 shall oblige the Supplier to disclose information if to do so would be in contravention of any applicable Data Protection Legislation or would require the Supplier to disclose confidential information relating to the Supplier's other clients in breach of a legally enforceable duty of confidentiality.

S3-20.7 The Supplier shall ensure that two back-up copies of the data and files used to support the Application and any other DfE Data (together, the "Backed Up Data") are made daily. The Supplier shall keep the first copy in a secure, fireproof physical location off site from the primary copy of Backed Up Data and the second copy in a secure, fireproof physical location at the same site as the primary copy of the Backed Up Data. As soon as reasonably practicable from the DfE's request from time to time and in any event prior to Mobilisation Acceptance, the Supplier shall also provide DfE with reasonable details of the protections it has put in place for transporting and storing media holding Backed Up Data off site.

S3-20.8 The Supplier shall ensure that the Backed Up Data is capable of being restored in the event of an Application system failure.

S3-20.9 The Supplier shall ensure that, in the event of a system failure, no more than four hours' worth of data, relating to the four hours immediately prior to the system failure, would be unrecoverable.

S3-20.10 The Supplier shall ensure that all media that hold Backed Up Data or copies of such data are transported in a secure manner, both internally within the Supplier's own organisation (and its Subcontractors' organisations) and externally. In the event that the Supplier wishes to transport such data externally:

S3-20.10.1 it shall use a reputable courier to do so, and shall also obtain signatures for both collection and delivery of such data; and

S3-20.10.2 it shall ensure that the Backed Up Data and any copies of it are securely encrypted.

S3-20.11 The Supplier shall test the capability to restore the Application from back up media (including copies of the Backed Up Data) prior to Mobilisation Acceptance and shall provide DfE with evidence of this capability.

S3-20.12 The Supplier shall test its capability to restore the Application from back up media (including copies of Backed Up Data) on a regular basis, and in any event at least once every six months.

S3-20.13 At the request of DfE, the Supplier shall restore or recreate any Backed Up Data that has been lost, corrupted or destroyed as a result of any Default by the Supplier. Such restoration or recreation shall be carried out promptly and at the Supplier's own cost. This right of DfE is in addition, and shall be without prejudice, to any other right or remedy of DfE whether under this Agreement or otherwise.

S3-20.14 The Supplier shall allow DfE staff and representatives to have access to the DfE Data and shall control such access to ensure that it does not compromise the integrity of any data.

S3-20.15 Without prejudice to any other rights and remedies of DfE, any breach of this Clause S3-20 by the Supplier that results in either a significant adverse effect on the reputation of DfE or on the reputation or integrity of the tests shall be a material breach of this Agreement.

S3-21. Disaster Recovery and Business Continuity

S3-21.1 The Supplier shall provide to DfE disaster recovery plans and business continuity plans ("Business Continuity Plans"):

S3-21.1.1 setting out clearly the conditions and circumstances under which the Business Continuity Plans will be invoked, outlining both the system recovery procedures to be followed in the event of a major system failure, including suitable redundancy and fail-over contingencies; and the alternative processes (including business processes) that the Supplier shall adopt in the event of disruption to Services;

S3-21.1.2 designed to prevent any loss of data prior to the date on which the disruption occurred to a maximum of four hours before the time of the last successfully completed transaction prior to the disruption occurring;

S3-21.1.3 designed to ensure that the Application is recovered within a maximum of 24 hours;

S3-21.1.4 addressing the various possible levels of failure or disruptions to Services, and the steps taken to remedy the different levels of failure and disruption;

S3-21.1.5 highlighting key contacts that the Supplier shall inform in the event of a failure or disaster, along with detailed recovery instructions, locations of any DfE Data or other data to be restored and any media or software;

S3-21.1.6 outlining the steps to be taken by the Supplier upon resumption of Services, such steps being designed to address any residual effect of the disruption (including a root cause analysis);

S3-21.1.7 designed to ensure that the DfE Security Requirements continue to be adhered to when such plans are invoked;

S3-21.1.8 in accordance with the minimum standards prescribed from time to time by any Regulatory Authority (including the Cabinet Office Security Policy Framework); and

S3-21.1.9 without limiting the generality of the foregoing, in accordance with Good Industry Practice.

S3-21.2 The Supplier undertakes that it has and shall continue to have in place and keep up-to-date such Business Continuity Plans. In addition:

S3-21.2.1 in the event of any material change to the Application, the supporting infrastructure or underlying business processes;

S3-21.2.2 after any invocation of the Business Continuity Plans; and

S3-21.2.3 on request from DfE from time to time,

the Supplier shall review and update, and provide DfE with a copy of: (a) the revised Business Continuity Plans (including the risk analysis upon which such plans are based); and (b) a report summarising the findings of the Supplier's review of the Business Continuity Plans, any changes in the risk profile of the Services and the Supplier's proposal for addressing the changes in such risk profile (including any proposed impact on the Services and Charges), for DfE's review. Following DfE's review of such materials, the Supplier shall amend the Business Continuity Plans in accordance with any recommendations by DfE that are reasonably required to ensure continuity of the Services and compliance with Clause S3-21.1.

S3-21.3 The Supplier shall not make any material changes to the Business Continuity Plans without DfE's prior written approval.

S3-21.4 The Supplier shall test the Business Continuity Plans to ensure their effectiveness prior to the Application being made available to Users (other than for the purposes of any tests relating to Mobilisation Acceptance) and when DfE reasonably requests such a test on the basis that there has been a material

change to the operational circumstances or business requirements of either Party. DfE shall have the right to attend and monitor any such tests. The Supplier shall also provide DfE with written results of any such testing and details of the steps taken to remedy any shortcomings or failings in the Business Continuity Plans identified as part of such testing.

S3-21.5 The Supplier shall work with DfE to ensure that its business continuity management arrangements align with DfE's business continuity strategy from time to time.

S3-21.6 Should a disaster or other event envisaged in the Business Continuity Plans occur and the Application is not Available, the Supplier shall notify DfE and shall ensure that, within one hour of the Application becoming not Available, an explanatory message shall be visible to Users attempting to view any of the pages on the Application. The Supplier shall ensure that it obtains the prior approval of DfE for any such explanatory message within one hour of the Application becoming not Available. For the purposes of this Clause S3-20.6, "Available" means that: (i) the Application is capable of accepting and processing incoming requests and data and responding to hyperlinks within pages; and (ii) Users can view all of the pages on the Application from the public internet in accordance with the Mandatory Requirements. Availability is measured at the point at which the Application interfaces with the public internet.

S3-21.7 Should a disaster or other event envisaged in the Business Continuity Plans occur, the Supplier shall notify DfE and carry out the Business Continuity Plans. In doing so, the Supplier shall not treat DfE any less favourably than any other service recipient of the Supplier.

S3-22. Co-operation

S3-22.1 The Supplier shall be open and co-operative and provide reasonable assistance to Regulatory Authorities, Users and any third party providing services to DfE in respect of national curriculum tests or any third party to whom DfE subcontracts or delegates any of its rights and obligations, or any other activities it undertakes as part of its business under this Agreement from time to time (each such third party being a "DfE Service Provider"). This assistance shall include:

S3-22.1.1 providing such information about the manner in which the Services are provided as is reasonably necessary for DfE Service Providers to provide their services to DfE or carrying out such activities as have been delegated to it by DfE;

S3-22.1.2 making available to, or accepting information from, Users, DfE Service Providers and Regulatory Authorities; and

S3-22.1.3 meeting DfE, Ofqual and other Regulatory Authorities and DfE Service Providers to discuss the Application and the websites and services provided by third parties.

S3-23. Employee Exit

NOT USED

S3-24. Conduct of Claims

S3-24.1 DfE shall notify the Supplier promptly in writing of any claim under Clause S3-2 (Intellectual Property Indemnity) and S3-23 (Employee Exit) of which it is aware, and shall not make any admission or take any other action which might be prejudicial to any proceedings without the express prior written consent of the Supplier (such consent not to be unreasonably withheld or delayed). The Supplier may conduct, at its own expense, any litigation and negotiations for a settlement of such claim. DfE shall give the Supplier all reasonable assistance required by the Supplier in support of any such defence or action.

S3-25. General

Publicity and Public Announcements

S3-25.1 The Supplier shall not make any public announcement or issue any circular relating to this Agreement without the prior written approval of DfE.

Further Assurances

S3-25.2 Each Party shall from time to time execute such documents and perform such acts and things as any Party may reasonably require to give full effect to the provisions of this Agreement and the transactions contemplated by it.

Waiver

S3-25.3 Not used, clause 12 of the Supplier's Terms and Conditions applies

Costs

S3-25.4 Each Party shall bear its own costs arising out of the negotiation, preparation and execution of this Agreement.

Amendment

S3-25.5 An amendment of this Agreement will not be binding on the Parties unless set out in writing, expressed to amend this Agreement and signed by authorised representatives of each of the Parties.

Notices

S3-25.6 Any notices to be given under this Contract shall be delivered personally or sent by post or by facsimile transmission to the Contract Manager (in the case of the Department) or to the address set out in this Contract (in the case of the Supplier). Any such notice shall be deemed to be served, if delivered personally, at the time of delivery, if sent by post, 48 hours after posting or, if sent by facsimile transmission, 12 hours after proper

Invalidity

S3-25.7 Not used, clause 13 of the Supplier's Terms and Conditions applies

Access to Information

S3-25.8 The Supplier shall hold, and permit DfE open access to, detail relating to all activities undertaken in delivering the Services.

Co-operation with Regulatory Bodies

S3-25.9 The Supplier shall cooperate with DfE in all requests for assistance in satisfying any requests for information from Ofqual or other Regulatory Bodies.

S3-26. Personnel

Standard of Staff

S3-26.1 The Supplier shall ensure that it provides (or has immediate plans to access) an adequate number of suitably qualified, skilled and experienced Personnel and shall ensure that they provide the Services with all due care and skill. In particular, all Personnel shall be fluent in English. Skills and qualifications of identified key personnel should cover all major aspects of the Service including commercial management, project management, technical skills and general management.

S3-26.2 The Personnel shall be thoroughly vetted by the Supplier in accordance with the DfE Security Requirements.

S3-26.3 For the avoidance of doubt, the Personnel shall not become employees of DfE and any instruction issued by DfE is issued to the Supplier and not directly to the Personnel.

Key Employees

S3-26.4 The Supplier shall agree with DfE which posts are considered as key posts, where knowledge or skills are critical to success.

S3-26.5 As at the Effective Date, the Supplier's key employees engaged in the provision of the Services are:

(i)

(ii)

(iii)

(the "Key Employees"). Upon DfE's reasonable request during the Term, the list of Key Employees in this Clause shall be amended to include any other Personnel which DfE considers to be Key Employees.

S3-26.6 If any of the Key Employees ceases to be involved in the provision of the Services, then the Supplier shall promptly nominate another employee of the Supplier to act as a Key Employee in place of that person. Prior to doing so, the Supplier shall:

S3-26.6.1 ensure that the individual has the appropriate ability and qualifications;

S3-26.6.2 notify DfE of its intention to appoint that individual;

S3-26.6.3 introduce the individual to appropriate representatives of DfE; and

S3-26.6.4 provide DfE with such information about the individual as is reasonably requested by DfE.

S3-26.7 If DfE reasonably and promptly objects in writing to the individual proposed under Clause S3-26.6, the Supplier shall not assign that individual to the position and shall propose to DfE another individual of suitable ability and qualifications. If DfE does not object to that individual, then they shall become a Key Employee for the purposes of this Agreement.

S3-26.8 All costs of training any replacement Supplier employee to act as a Key Employee, or other handover costs, shall be borne by the Supplier.

S3-26.9 The Supplier shall ensure any resource related risks are documented within the Risk Log.

Removal of Personnel

S3-26.10 DfE may require the Supplier to remove any Personnel from the provision of the Services where it can demonstrate reasonable grounds for that Personnel's unsuitability. If any Personnel are removed, the Supplier shall as soon as reasonably practicable replace them with suitable alternatives.

Solicitation of Employees

S3-26.11 Neither Party shall, and each Party shall ensure that its Group Companies shall not, at any time during the Term or for 12 months after termination of this Agreement, solicit or endeavour to entice away from or discourage from being employed or hired by the other Party or its Group Companies any person who is an employee of the other Party or its Group Companies and who, to that Party's knowledge, is or was engaged in the Services in the previous 12 months whether or not such person would thereby commit a breach of his contract of service and save that this restriction shall not apply to any person who has received a notice of redundancy or dismissal.

S3-26.12 The restrictions in Clauses S3-26.11 shall not apply if a person who is or was an employee of a Party is employed as a result of a response by that person to a public advertisement.

S3-27. Sub-Contractors

S3-27.1 The Supplier shall demonstrate that, where there are plans to use a Subcontractor, the Subcontractor is reliable, available and can meet the obligations imposed on the Supplier under this agreement. The Supplier shall provide and maintain details of who these resources are, how they will be used and how they will be managed. The Supplier shall provide DfE with its procurement strategy and selection criteria for all Services which they intend to Subcontract. The Supplier shall advise DfE of the progress of its procurement activities against the agreed plan and inform DfE of the nominated preferred bidder prior to contract award.

S3-27.2 The Supplier shall require that any subcontractor(s) are operating acceptable security policies, in line with the Cabinet Office Security Policy and shall confirm that this is the case prior to letting the relevant subcontract(s). The Supplier shall provide DfE with copies of a completed Security Policy Framework matrix for each Subcontractor. The Supplier shall procure that its Subcontractor agree to security audits by DfE where required.

S3-28. Charges

S3-28.1 Charges are as stated in the G-Cloud Digital Marketplace and confirmed by the Supplier, as its standard pricing, on 23rd October 2015.

S3-28.2 These charges are detailed in Schedule 3 of the Supplier's terms and Conditions and Appendix 1 of this Section 3.

S3-29. Accounts and Audit

S3-29.1 The Supplier shall maintain full and accurate accounts for the Service against the expenditure headings in the Table. Such accounts shall be retained for at least 6 years after the end of the financial year in which the last payment was made under this Contract. Input and output VAT shall be included as separate items in such accounts.

S3-29.2 The Supplier shall permit duly authorised staff or agents of DfE or the National Audit Office to examine the accounts at any reasonable time and shall furnish oral or written explanations of the accounts if required. DfE reserves the right to have such staff or agents carry out examinations into the economy, efficiency and effectiveness with which the Supplier has used DfE's resources in the performance of this Contract.

S3-30. Invoices

S3-30.1 Invoices shall be prepared by the Supplier monthly in arrears and shall be detailed against the expenditure headings set out in the Table. The Supplier or its nominated representative or accountant shall certify on the invoice that the amounts claimed were expended wholly and necessarily by the Supplier on the Service in accordance with the Contract and that the invoice does not include any costs being claimed from any other body or individual or from the DfE within the terms of another contract.

S3-30.2 Invoices shall be sent, within 30 days of the end of the relevant month, to SSCL Accounts Payable Team, Room 6124, Tomlinson House, Norcross, Blackpool FY5 3TA, quoting the Contract reference number. The DfE undertakes to pay correctly submitted invoices within 5 days of receipt. The DfE is obliged to pay invoices within 30 days of receipt from the day of physical or electronic arrival at the nominated address of the DfE. Any correctly submitted invoices that are not paid within 30 days may be subject to the provisions of the Late Payment of Commercial Debt (Interest) Act 1998. A correct invoice is one that: is delivered on time in accordance with the contract; is for the correct sum; is in respect of goods/services supplied or delivered to the required quality (or which are expected to be at the required quality); includes the date, supplier name, contact details and bank details; quotes the relevant purchase order/contract reference and has been delivered to the nominated address. If any problems arise in relation to invoicing matters the Supplier shall contact the DfE's Contract Manager. The DfE shall aim to reply to any complaint within 10 working days. The DfE shall not be responsible for any delay in payment caused by incomplete or illegible invoices.

S3-30.3 The Supplier shall have regard to the need for economy in all expenditure. Where any expenditure in an invoice, in the DfE's reasonable opinion, is excessive having due regard to the purpose for which it was incurred, the DfE shall only be liable to reimburse so much (if any) of the expenditure disallowed as, in the DfE's reasonable opinion after consultation with the Supplier, would reasonably have been required for that purpose.

S3-30.4 If this Contract is terminated by the DfE due to the Supplier's insolvency or default at any time before completion of the Service, the DfE shall only be liable under Appendix 1 of this Section 3 to reimburse eligible payments made by, or due to, the Supplier before the date of termination.

S3-30.5 On completion of the Service or on termination of this Contract, the Supplier shall promptly draw up a final invoice, which shall cover all outstanding expenditure incurred for the Service. The final invoice shall be submitted not later than 30 days after the date of completion of the Service.

S3-30.6 The DfE shall not be obliged to pay the final invoice until the Supplier has carried out all the elements of the Service specified in this Agreement.

S3-30.7 It shall be the responsibility of the Supplier to ensure that the final invoice covers all outstanding expenditure for which reimbursement may be claimed. Provided that all previous invoices have been duly paid, on due payment of the final invoice by the DfE all amounts due to be reimbursed under this Contract shall be deemed to have been paid and the DfE shall have no further liability to make reimbursement of any kind.

S3-31. Change Control

S3-31.1 The Change Control Process is detailed in Schedule 4 of the Supplier's Terms and Conditions.

S3-31.2 The parties have agreed to use the model Change Control Note at Appendix 2 to Section 3.

S3-32. Quality and Technical Standards

Standards and Methodologies

S3-32.1 The Supplier shall adhere to relevant standards and methodologies which shall include, but not be limited to:

S3-32.1.1 ISO9001: Quality Management System

S3-32.1.2 ISO/IEC 27001: Information Management Security System

S3-32.1.3 BS 25999 or ISO 23301: Business Continuity Standard

S3-32.1.4 ISO/IEC 24762: IT Disaster Recovery

S3-32.1.5 HMG Security Policy Framework (SPF), version April 2014

S3-32.1.6 PRINCE2 (Projects in controlled Environments)

S3-32.1.7 ITIL (Information Technology Infrastructure Library)

S3-32.1.8 MoR (Management of Risk)

S3-32.2 The Supplier shall ensure that its solution for the delivery of the service meets the DfE's information standards, see points 1-3 below, and is flexible enough to support new and updated standards, as notified by the DfE, as and when they are published. The Supplier shall ensure that their systems follow the principles of data management – ensuring that master copies are held and accessible in emergency.

S3-32.3 The Supplier shall ensure that any data that is presented for transfer, between the Supplier and DfE, is in a format agreed by DfE and shall ensure that all data feeds are technically compliant with the Common Basic Data Set (CBDS), see point 4 below.

References:

1. https://data.gov.uk/education-standards/about-isb
2. https://data.gov.uk/education-standards/standards
3. https://data.gov.uk/education-standards/papers
4. https://www.gov.uk/government/collections/common-basic-data-set

S3-32.4 The Supplier shall provide DfE and/or its nominated representative(s) access to the Application.

Technical Requirements for the current applications

S3-32.5 The Supplier shall ensure that the .NET platform and Source Code written in C# and HTML5 as appropriate is maintained.

S3-32.6 The Supplier shall ensure that the Application shall utilise an SQL 2008 R2 database. Additionally, the Supplier shall be able to demonstrate the capability to upgrade from SQL 2008 R2 to a later version of SQL.

S3-32.7 The Supplier shall at all times maintain all documentation associated with the Application and which meets an Industry Accepted Standard. The Supplier shall provide copies of the documentation to DfE at any time on request.

S3-32.8 The Supplier shall provide a duplicate of any external facing system (a test environment) for the use of DfE The Supplier shall ensure a test environment that mirrors the Production environment in regards to configuration, for example the same Operating System and Database versions.

S3-32.9 The Supplier shall retain all DfE data and maintain its integrity until handover to DfE at the end of the contract term or ensure its secure destruction, providing evidence to DfE to confirm this action.

S3-32.10 The Supplier shall continue to ensure that Access Control is enforced such that the appropriate user can access the appropriate function within the Application. This includes the addition and removal of users from the Application.

S3-32.11 The list of users will not be limited to DfE employees and may include representatives of DfE, other DfE service providers and other relevant stakeholders.

S3-32.12 The Supplier shall allow appropriate DfE staff to have access to the raw data contained within the Application: access will be controlled to ensure that it does not compromise data integrity.

S3-32.13 The Supplier shall ensure that any future Development shall support web accessibility and is (at a minimum) compliant with AA of the W3C Web Content Accessibility Standards, see references below.

S3-32.14 The Supplier shall seek independent accreditation of its solution and provide evidence in terms of a certificate or statement of compliance to DfE.

S3-32.15 The Supplier shall ensure that any future Development shall support web accessibility and is (at a minimum) compliant with AA of the W3C Web Content Accessibility Standards.

Development, Testing and Deployment

S3-32.16 The development, testing and deployment of the Application shall be controlled under best practice Configuration Management arrangements through the provision of tools and processes for configuration control aligning with ITIL v3 best practice, or equivalent. This includes:

S3-32.16.1 Maintenance of a configuration library containing all items under configuration control

S3-32.16.2 Maintaining version control for all configuration items

S3-32.16.3 Testing and release management processes

S3-32.17 Any changes to the Application shall undergo rigorous testing before its introduction into Live Service.

S3-32.18 The Supplier shall produce a testing strategy and associated plan for the delivery of any changes to the Application that shall be subject to review and sign off by DfE.

S3-32.19 Testing shall cover the functional and non-functional requirements;

S3-32.19.1 The supplier shall be obliged to consider feedback from DfE User Acceptance Testing activities and implement changes as necessary;

S3-32.19.2 If for any reason a change is made to the Application post-assurance then the Supplier shall provide evidence of a full regression test as well as targeted testing for the change;

S3-32.19.3 The Supplier shall ensure that the Application will be penetration tested by a CESG accredited company by a date to be agreed with DfE. The penetration test report is to be provided to DfE along with any proposed remedial action for issues contained within the report.

S3-32.19.4 The Supplier shall load test the Application using either an independent third party or internally using an Industry Accepted Standard load testing tool. The Supplier shall ensure that the strategy and parameters for the load testing are agreed in advance with DfE before any load testing is carried out and provide the results of the load testing to DfE.

S3-32.20 The Supplier shall provide appropriate Industry Accepted Standard evidence of their internal testing, addressing functionality, capacity, security, performance, availability and resilience, including but not limited to:

S3-32.20.1 Test scripts

S3-32.20.2 Defect report

S3-32.20.3 System sign-off documents

S3-32.20.4 Deployment report

S3-32.20.5 Load test report

S3-32.20.6 Penetration test report

S3-32.21 The Supplier shall host the Application on a domain or sub-domain as specified by DfE and will support any transition to a single government domain that may be required in the future.

S3-32.22 The Supplier shall ensure that the Application is capable of connecting to external applications (e.g. Pupil Registration) using the Single Sign on solution.

Quality

S3-32.23 The Supplier shall ensure that all project staff engaged in the delivery of the Services have a level of knowledge of the contractual terms and conditions commensurate with the level of their responsibility and involvement

S3-32.24 All Supplier website design for the application delivery shall conform to the DfE identity guidelines and information architecture. The Supplier shall ensure that the Website echoes the look and feel of the main STA website and is agreed with the DfE prior to implementation. The Supplier shall work with DfE to ensure that its website design integrates with DfE's application framework.

S3-33. Exit Management

Documentation

S3-33.1 The Supplier shall, at no cost to DfE, ensure that the following documentation is available for the Application and describes the architecture and components in sufficient detail that any successor operator or users not involved in the initial development can use, install, operate and maintain the Application. This should include but not be limited to:

S3-33.1.1 A design document with architectural diagrams describing the solution infrastructure;

S3-33.1.2 Interface documentation containing details of interfaces to other elements of the Application and modules where information is shared;

S3-33.1.3 A technical specification document defining the technical aspects of the Application, including the standards to which they have adhered (noting that the Cabinet Office guidelines insist that procured Application are based upon recognised open standards where they exist);

S3-33.1.4 A functional specification document or equivalent defining the functional operation of the Application; and

S3-33.1.5 Documentation of operation and user processes.

S3-33.2 The Supplier shall put in place the necessary measures to keep this documentation up to date and available to DfE on request and in accordance with the agreement.

S3-33.3 The Supplier shall provide and maintain a detailed, fully resourced and costed exit and transition plan to ensure the smooth transition of Services to a Successor Service Provider.

S3-33.4 The Supplier shall provide a detailed statement in the Exit and Transition Plan of all its requirements for the support it requires from DfE to ensure a smooth transition of Service to a Successor Service Provider at the expiry or termination of the Framework.

S3-33.5 The Supplier shall provide a full Warranty on the Application and associated documentation for a period of 6 months following expiry or termination of the contract.

Exit and Transition Plan

S3-33.6 The Supplier shall produce, at no cost to DfE, an Exit and Transition plan within three months of the Effective Date.

Transition

S3-33.7 Where the provision of the New Services constitutes a relevant transfer under TUPE (and in the event of doubt, DfE's determination as to the applicability of TUPE shall be final and binding on the Supplier):

S3-33.7.1 the parties shall co-operate to ensure that the requirement to inform and consult with the Transitioning-Out Personnel and employee representatives in relation to any relevant transfer under TUPE is met;

S3-33.7.2 the Supplier shall perform and discharge all its obligations in respect of all the Transitioning-Out Personnel and their representatives up to and including the Contract End Date.

Exit

S3-33.8 The Exit Service is an extension to the Services that:

S3-33.8.1 ensures the smooth transition of some or all of the Services and the Transitioning-Out Personnel to any New Supplier; and / or

S3-33.8.2 runs down some or all of the Services; and / or

S3-33.8.3 undertakes the Supplier's obligations to transfer property and / or make data and / or information available to DfE in accordance with this Agreement; and / or

S3-33.8.4 identifies individuals that may transfer into new employment by operation of law as a result of the transfer of some or all of the Services (and full details of those individuals) as set out in clause S3-2.1; and / or

S3-33.8.5 identifies goods and intellectual property rights that are owned by DfE, which are under the control of the Supplier or its subcontractor(s), for delivery to DfE and / or a nominated third party; and/ or

S3-33.8.6 identifies goods and intellectual property rights that are not owned or licensed by DfE, which are under the control of the Supplier or its subcontractor(s) ("Third Party Goods and Rights"), and

S3-33.8.7 subject to clause S3-27.7, grant (or use reasonable endeavours to grant (as the case may be)) rights of use for the Third Party Goods and Rights to DfE as may be reasonably necessary to transition the Services to DfE and / or a new supplier subject to full payment therefore.

S3-33.9 The Exit Service will be defined in detail by the parties as a variation in accordance with clause S3-33 or, if the parties do not agree the Exit Service as a variation (for example, if it is impractical to complete the formalities set out at clause S3-33 in the limited timescales), as reasonably requested by DfE in writing and in accordance with DfE's reasonable instructions.

S3-33.10 The Supplier shall deliver to DfE the Created Source Code to the extent not already delivered to DfE under this Agreement in such electronic formats as DfE may reasonably require or accept.

S3-33.11 The Supplier shall provide DfE with all reasonable cooperation and assistance to effect transition of the Services in accordance with DfE's reasonable instructions. Clauses S3-18 to S3-19 shall continue in force for the duration of the Exit Service.

S3-33.12 The Supplier commits to granting to DfE the rights of use required by clause S3-27.2 on commercially reasonable terms. If commercially reasonable terms are not agreed, the terms shall be resolved in accordance with the provisions of clause S3-33.

S3-33.13 The provisions of clauses S3-27.2 and S3-27.6 shall not apply to the Orderline Website (or the intellectual property rights therein) or to any other third party Intellectual Property Rights that have been: (i) identified by the Supplier to DfE in writing as being part of the Services; and (ii) acknowledged as such by DfE in this Agreement or in a Change Control Note.

S3-34. Time is of the Essence

S3-34.1 For the avoidance of doubt, time is of the essence of this contract.

Appendix 1 - Charges

CHARGES FOR THE SERVICES ARE BASED ON THE FOLLOWING ENVIRONMENTS:

LIVE ENVIRONMENT		
Front End	**Database**	**Management Server**
4 x load-balanced web frontend servers	1 x Server database server	1 x Management server (Backups, AV)
2 physical CPU's with 12 cores per CPU	2 x CPU's	4 CPU's per server
32GB RAM per server	16 x Gb RAM	4 Gb RAM
Storage (avg.) 300Gb	Storage 508Gb	Storage 350Gb
FAILOVER ENVIRONMENT		
Front End	**Database**	**Management Server**
1 x web frontend server	1 x Server database server	1 x Management server (Backups, AV)
2 x CPU's	2 x CPU's	2 CPU's per server
2 x Gb RAM	48 x Gb RAM	2 Gb RAM
Storage 70Gb	Storage 640Gb over two drives	Storage 700 Gb
TEST/STAGING ENVIRONMENT		
Front End	**Database**	**Management Server**
1 x web frontend server	1 x Server database server	None
2 x CPU's	2 x CPU's	
2 x Gb RAM	16 x Gb RAM	
Storage 60Gb	Storage 240Gb	

Monthly Charges are as follows:

Description	Price (excl VAT)	Price (incl VAT)
1. Set-up costs	-	-
2. Hosting services (per month)		
3. Maintenance services (per month)	-	-
4. Support Services (per month)		
Fixed Cost (19 May 2017 – 19 May 2019)		

The Standard rate card is as follows:

	Strategy & architecture	Business Change	Solution Development & Implementation	Service Management	Procurement & Management Support	Client Interface
1. Follow	550	N/A	550	450	N/A	450
2. Assist	650	650	650	550	550	550
3. Apply	750	750	750	650	650	650
4. Enable	850	850	850	750	750	750
5. Ensure/Advise	1,000	1,000	1,000	850	850	850
6. Initiate/Influence	1,300	1,300	1,300	1'000	1'000	1,000
7. Set Strategy/Inspire	1,600	1,600	1,600	1,300	1,300	N/A

Standards for Consultancy Day Rate cards

Consultant's Working Day – 8 hours exclusive of travel and lunch.

Working Week – Monday to Friday excluding national holidays

Office Hours - 09:00 – 17:00 Monday to Friday

Travel and Subsistence – Included in day rate within M25. Payable at department's standard T&S rates outside M25.

Mileage – As above

Professional Indemnity Insurance – included in day rate.

Appendix 2 – Model Change Control Note

CHANGE CONTROL NOTE (CCN) – No [To be allocated by STA]			
Contract name & No:			
Originator:			
Date of CCN:		**Expiry date:**	
CCN Title			
1. Reason for change:			
2. Details of change (including specification where appropriate):			
3. Price (if appropriate) to include cost breakdown and payment schedule:			
4. Implementation timetable:			
5. Impact of the change on the Services:			
6. Required changes to the Contract (Clauses and Schedules):			
7. Authorised to sign for and on behalf of the Supplier:			
Signature:			
Name in CAPITALS:			
Position in Organisation:			
Date:			
8. Authorised to sign for and on behalf of the DfE:			
Signature:			
Name in CAPITALS:			
Position in Organisation:			
Date:			

INTRODUCTION:

(A) These Supplier Terms ("Terms") shall form part of the Supplier's Tender. Unless defined specifically in these Terms, any defined terms shall have the meanings set out in the Framework Agreement and/or the Call-Off Agreement, which shall be incorporated into these Terms.

(B) These Terms are subject to the Framework Agreement and Call-Off Agreement and any conflict or ambiguity between the Framework Agreement, the Call-Off Agreement and these terms shall be resolved in accordance with CO-1 of the Call-Off Agreement.

Schedule 1: Hosted Services

Service Level Commencement Date	19/05/2017
Availability	
Backups	
External Monitoring	
Usage Statistics	
Scheduled Maintenance	

See also Annex 1C to the Order Form for further detail on Service Management, Service Levels and Service Credits.

Schedule 2: Support Services

Service Level Commencement Date	19/05/2017
Helpdesk Service	
Helpdesk Service Hours	
Logging Issues	
Service Levels	

See also Annex 1C to the Order Form for further detail on Service Management, Service Levels and Service Credits.

Schedule 3: Fees

Development Services

	Strategy & architecture	Business Change	Solution Development & Implementation	Service Management	Procurement & Management Support	Client Interface

1.	**Follow**	550	N/A	550	450	N/A	450
2.	**Assist**	650	650	650	550	550	550
3.	**Apply**	750	750	750	650	650	650
4.	**Enable**	850	850	850	750	750	750
5.	**Ensure/Advise**	1,000	1,000	1,000	850	850	850
6.	**Initiate/Influence**	1,300	1,300	1,300	1’000	1’000	1,000
7.	**Set Strategy/Inspire**	1,600	1,600	1,600	1,300	1,300	N/A

Hosting Services

Monthly cost to host the application in an IL3 environment, available 365 days per year with a minimum 99.80% availability for the 'live' system, including failover:

Cost also includes the hosting of the test/stage environment with a minimum availability of 98% - there is no requirement for the test/stage environment to be supported by a failover.

Support Services

Monthly cost for providing Technical Support Desk & Incident Management (using ITIL v3.0) to the Systems team of STA:

Schedule 4: Change Control Procedure

Introduction

1. This Schedule outlines the arrangements for making changes to this Agreement.

Principles

2. Each party shall bear its own costs in complying with all procedures set out in this Schedule 4. For the avoidance of doubt, and without prejudice to any change to the Fees that may be agreed between the parties pursuant to the provisions of this Schedule 4, Customer and TSO agree and acknowledge that the work carried out by TSO in accordance with all procedures of this Schedule 4 is at no additional cost to Customer.

3. Subject to paragraph 4 of this Schedule 4, where Customer or TSO see a need for a change under this Agreement pursuant to clause 8, Customer may at any time request and TSO may at any time recommend such a change only in accordance with the change control procedures as set out in this Schedule 6 (the "Change Control Procedure").

4. Any changes subject to this Schedule 4 shall be agreed between the parties in writing by the authorised representatives of both parties. Neither Customer nor TSO shall unreasonably withhold or delay its agreement to any such change.

5. Subject to paragraph 4 of this Schedule 4, until such time as a change is agreed and takes effect in accordance with this Change Control Procedure:

    (a) TSO shall, unless otherwise agreed in writing by the authorised representatives of both parties, continue to perform the Services as if the request or recommendation had not been made; and

    (b) Customer shall, unless otherwise agreed in writing by the authorised representatives of both parties, continue to pay any Fees properly due in accordance with this Agreement as if the request or recommendation had not been made;

6. Any discussion which may take place between Customer and TSO in connection with a request or recommendation before the authorisation of a resultant change to the Services shall be without prejudice to the rights of either party.

7. Any work undertaken by TSO or an Approved Sub-Contractor which has not been authorised in advance by Customer and in accordance with the provisions of this Schedule 4 shall be undertaken entirely at the expense and liability of that party.

Procedures

8. A change proposal form ("CPF") shall be raised by either party to facilitate discussion between Customer and TSO concerning a change to the Agreement. Each CPF shall be in the form set out in Annex 1 to this Schedule 4.

9. The CPF should include as a minimum the following information:

    (a) the reason for the proposed change;

    (b) the originator and planned date for proposed change;

    (c) the proposed amendments to the text within the appropriate clauses, Schedules, Annexes and Appendices; and

    (d) an assessment of the impact on other clauses, Schedules, Annexes and Appendices.

10. Upon receipt of a CPF from either party, the other party shall have up to ten (10) Business Days (or such other reasonable period as may be agreed by the parties) to consider the CPF following which the parties shall meet (which may be on more than one occasion) to discuss the relevant CPF.

11. Such discussion shall result in either:

    (a) no further action being taken on the CPF; or

(b) agreement between the parties on the change to be made (including changes to this Agreement and including the date upon which the changes are to take effect), such agreement to be expressed in the form of proposed revisions to the relevant parts of the Agreement.

12. A copy of any proposed revisions to this Agreement agreed between the parties (referencing the relevant CPF prepared in accordance with this Schedule 4) that are agreed in writing and accompanied by a completed CPF signed by the authorised representatives of both parties shall constitute a variation to this Agreement ("Contract Variation").

13. A Contract Variation made pursuant to this Schedule 4 shall not be effective to amend the Agreement unless it includes the amended text of any clauses, Schedules, Annexes or Appendices affected by the agreed change.

14. Any discussions, negotiations, or other communications which may take place between Customer and TSO in connection with any proposed change to this Agreement, including but not limited to the submission of any written communications prior to the signing by both parties of the relevant Contract Variation shall be without prejudice to the rights of either party.

Annex 1 to Schedule 4

Each CPF shall contain:

- a unique identifier;
- the title of the change;
- the name of the originator and date of the request or recommendation for the change;
- the reason for the change;
- full details of the change including any specifications and the timeline for delivery;
- the Fees, if any, to be made for the change including all one-off (nonrecurring) Fees;
- a timetable for implementation together with any proposals for acceptance of the change;
- a schedule of payments (if appropriate);
- details of the likely impact, if any, of the change on other aspects of the Agreement and/or the service specification including but not limited to:
    - the term of this Agreement;
    - impact of any benefits realisation;
    - the Fees;
    - the Services;
    - the payment terms;
    - the responsibilities of Customer and TSO; and
    - Service Levels;
- such other information as the party raising the CPF reasonably regards as relevant; and
- provision for Customer and TSO to record the progress with dates of the CPF for each stage as follows:
    - submitted;
    - further information required;
    - further information received;
    - revised CPF received;
    - consideration, discussion and agreement to the CPF; and
    - all proposed amendments to the Clauses and Schedule of the Agreement.

See Appendix 2 of Section 3 for the model Change Control Note.

2.

Schedule 5: Acceptance Certificate

<Project Name and reference>

This Acceptance Certificate refers to:

Project Name & No:	
Milestone Name	
Milestone Delivery Date	
Author(s):	
Date:	
Version:	
Distribution:	

This is to confirm that the above work has been accepted.

Accepted: YES/NO

DATE:

_____

AUTHORISED SIGNATURE

_____

Schedule 6: Implementation Plan

Milestone	Milestone Date	Requirement
Exit Plan	22/08/2017	The document should detail how the Supplier will manage the exit from the contract including, but not limited to; • Identifying potential risks and/or issues to exit and how these could be mitigated • Proposals for how the Supplier would support different exit routes for example transfer to new supplier, moving to in-house provision etc. • Should cover termination through dispute as well as contract running for full term • What the Supplier's expectations would be in terms of required input from the Customer.
Business continuity plan	22/08/2017	The document should detail how the Supplier will manage an incident that impacts normal service operation beyond standard support capabilities and should include, but not be limited to; • Single site failure, how the service will be maintained should a single site be unavailable • Single site failure, how the service support will be maintained should a single site be unavailable • Multiple site failure, how the service will be maintained should multiple sites be unavailable • Multiple site failure, how the service support will be maintained should multiple sites be unavailable • Include any potential risks and/or issues that may result in an incident that would impact normal service operation.
Disaster recovery plan	22/08/2017	The document should detail how the Supplier will manage an incident that impacts normal service operation beyond standard support capabilities. It should look to cover the items listed in the Business continuity plan, and may be included as a single document. However this should allow for more significant incidents that the business continuity plan alone.
Service plan	22/08/2017	The document should include how the service will be supported and should include, but not be limited to; • Defined support windows provided by the Supplier • Definition of the service being supported • The resources required to support the service • Any dependencies that are required to allow the service to be available and/or supported

		• Tools used in the support of the service • Processes used in the support of the service • Known major developments/upgrades that will, or could, impact the service
Project initiation document	22/06/2017	The document should detail the work that is currently ongoing and how that work will be managed and transitioned to the new contract. It should also define work that will be completed and invoiced under the existing agreement (STA0060). There should also be a plan included showing how the timescales of when the work will be transitioned.
Security document	22/08/2017	The document should detail how the Supplier will ensure that they are compliant with the Customer's security policies. This will also cover any accreditations that provide evidence that processes currently utilised by the Supplier meet the required standards.
Service guide	22/08/2017	The document should detail how the service will be managed and will include, but not be limited to, the following; • Technical overview of the system being supported • Incident reporting and management procedures • Service level agreements and service credit calculations and procedures • Management information and reporting definitions • Change management procedures • Escalation procedures and key contacts.