Crown Commercial Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Table of Contents

Part A: Order Form

Digital Marketplace service ID number	7714 0531 8027 441
Call-Off Contract reference	Con_10043
Call-Off Contract title	Research Evidence Directory Portal
Call-Off Contract description	The Department for Education (the Department) is seeking to establish a Contract for a single portal simplifying access to a range of research services and information, containing (among other capabilities) an interactive research repository or directory (RED). The system will need to be integrated, easy to use, accessible and secure.
Start date	07 June 2021
Expiry date	06 June 2023
Call-Off Contract value	£257,000
Charging method	BACS
Purchase order number	[redacted]

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
To the Supplier	Altiar Limited Unit 8 1st Floor Jason House Kerry Hill Horsforth Leeds LS18 4JR Company number: 09117182
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Chief Social Researcher and Deputy Director for DfE Central Research Division

Name: [redacted]

Email [redacted]

For the Supplier:

Title: CEO

Name [redacted]

Email: [redacted]

Phone: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 7 June 2021 and is for **24 months**.
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for 2 period(s) of up to 12 months each, by giving the Supplier 4 weeks written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot	This Call-Off Contract is for the provision of Services under: • Lot 2: Cloud Software
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: • Service ID: 7714 0531 8027 441 • Link to Service Descriptions: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/771405318027441 • Link to Service Definition: https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/702290/771405318027441-service-definition-document-2020-07-13-1540.pdf The Supplier will provide DfE with a research evidence directory. This system will act as a central place for DfE staff to search both the internal and external evidence base and to find information about research which is currently live (both internal and where possible externally funded). The portal will act as a 'one stop shop' for information on DfE research evidence services, as well as drawing together relevant research information. The portal should allow users to quickly and easily: • explore robust relevant research evidence (whether DfE funded or externally funded), • learn more about research (not only DfE research), aiding co-ordination, • help them confidently identify genuine gaps in the evidence base, and get help with filling them, • build research skills (both for analysts and non-analysts) • find details about relevant research associates and Suppliers.
Additional Services	Additional functionality may be agreed at a later date. Where additional functionality is required, the Department expects the Supplier to work to and agree an implementation timetable. If any of these requirements incur additional costs, a contract variation will be issued to the Supplier.

	All Services will be as detailed in the order form.
Location	The Services will be delivered to Department for Education Sanctuary Building Great Smith Street London SW1P 3BT
Quality standards	The quality standards required for this Call-Off Contract are: • As set out in the Call Off Contract; and • As expected from good industry practice and the Supplier's published service definition under the service reference stated at the head of this order form. • As set out in the customers policies and quality standards as listed in Table 1 of Schedule 1 in addition to the Call-Off terms section of this order. • The portal must look modern, visually appealing and be simple for users to navigate.
Technical standards:	The technical standards used as a requirement for this Call-Off Contract are as detailed in the relevant Service Description and documents on the G-Cloud 12 Framework for Service ID: 7714 0531 8027 441. **Cyber Essentials Certification:** Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. Supplier to follow the technology code of practice Technology Code of Practice - GOV.UK (www.gov.uk) when designing and building government services and meeting GDS service standards.

Service level agreement:	The service level and availability criteria required for this Call-Off Contract are as detailed and published within the Service description and definition for Service ID: 7714 0531 8027 441. This may include any specific service levels or availability criteria required in the delivery of the services. You can only use the service levels or availability criteria: • in the Supplier's Service Definition • in the Service Description • used as a requirement or acceptance criteria. The Supplier should use the following process to manage; • **Incident / issues / faults** o SLAs - with a hybrid hosting approach; to ensure we provide the business with consistent approach to incident SLA management, The Supplier should adopt and agree to commit to the DfE standard SLAs and definitions, as below. o The business should utilise the Altiar ServiceDesk to report incidents / issues / faults. o If, upon Supplier triaging an incident, Supplier to determine the issue lays with the DfE hosting; Supplier should be responsible for raising the required ticket for DfE InfraOps support via the DfE ServicePortal. This will ensure the quickest time to resolution, ensure correct technical details are included within the DfE INC ticket and ensure that DfE and Altiar technical personal are able to converse directly as required to resolve any issues and test fixes etc. o Have Altiar state their support hours. Altiar's support hours should be detailed in the contract. • **Major incident management** o Supplier to utilise the DfE Major Incident Management process and team to co-ordinate on any major incidents. o In turn; utilise the DfE Problem Management process and team. o The Supplier is required to engage with the DfE MIM and PM processes.

The Supplier should use all reasonable endeavours to respond to the Buyer's SLA's as set out below.

Triage may take longer than 20 minutes in exceptional circumstances. In the event a triage takes longer than what is outlined within the SLA, the Supplier will notify the Buyer's Contract Manager.

DfE Incident SLAs

Priority (Incident)	Triage Time	Target Update	Total Fix Time (working hours)
Priority 1 (P1) - Major Incident	20 minutes	Every hour	4 hours
Priority 2 (P2) - Significant	20 minutes	Every 4 hours	8 hours
Priority 3 (P3) - Minimal	20 minutes	Every 2 days	24 hours
Priority 4 (P4) - Negligible	20 minutes	On request	5 days

DfE Request SLAs

Priority (Request)	Triage Time	Target Update	Total Fulfilment time (working hours)
Priority 3 (P3)	20 minutes	On request	5 days
Priority 4 (P4)	20 minutes	On request	30 days

DfE SLA Definitions

Example of service enhancement requests

Simple	Eg – adding / amending / removing fields	These CHGs will be made by the Altiar CRM / DB Admin users. We do not anticipate that changes in this category will require extensive analysis or CHG governance.

	within forms	
Intermediate	Eg – adding / amending hard-coded validation rules	These CHGs will be made by the supplier. We do not anticipate that changes in this category will require extensive analysis or CHG governance. The SLA is for the delivery of the CHG within 5 working days of the request.
Complex	Eg. The development of new functionality etc	These CHGs will be made by the supplier. Changes in this category may require business analysis, project management, more extensive testing and the contribution towards CHG governance. The SLA is for the investigation and agreement with DfE of an estimate for delivery within 5 working days of the request.

Altiar Support

Support for the Altiar Enterprise platform covers queries and issues when using the software, the deployment and configuration of the system and enhancement / feature requests. Altiar offer comprehensive support across these areas with a clearly defined set of support channels, request processes, and issue submission and resolution guidelines.

Requests

Usually, a support request will be raised for one of two reasons: to resolve an issue that a user or organisation is experiencing or to request an enhancement to the system. Both request types share the same channels and submission definitions, but the progression and resolution processes differ between the two. In the scope of this document the term ‘support request’ applies to both issues experienced when using Altiar and any requests for functional enhancements. Issues are reviewed as near to the time of submission as possible, categorised by type and then progressed through the online support system. Enhancement requests are acknowledged and then added to an internal roadmap for review and possible inclusion in a future release of Altiar. Raising a feature request does not guarantee its inclusion but Altiar aim to accommodate these requests wherever possible.
To facilitate the submission and feedback of support requests, an online support and issue tracking system is provided. Requests can be submitted to the system simply by emailing support@altiar.com or by raising a ticket through the support centre itself. An area is provided within the support centre where you can view and manage all your existing support requests.

Resolution

Support requests are internally categorised into one of four priority states (see table below) which carry varying resolution target times. Although Altiar strive to always meet or exceed these resolution times, they are for informational purposes only and are not guaranteed to be met.

Urgent	Critical Issues with complete application failure	6 hours from
High	Application issue resulting in substantial loss of functionality	24 hours from
Medium	Application issue resulting in some loss of functionality	48 hours from
Low	Feature or Change Request	Reviewed on a ca by-case basis

Contact

The Altiar online support centre allows you to raise a support request and this is the best way to contact Altiar for support. It ensures that the request can be categorised, tracked and resolved efficiently and exposes the request to the maximum number of support staff at any given time. You can easily submit a request to us by emailing support@altiar.com

Onboarding

The onboarding plan for this Call-Off Contract is

Milestone	Notes	Start Week	End Week
Project kick off meeting	Meeting with DfE stakeholders to discuss requirements for page / filter structure, branding / layout and site content	1	1
Technical requirements discussion	Meeting with DfE technical team to discuss requirements for security, domain,	1	1

		SSO implementation		
	Site deployment	Altiar to provision site and provide initial login credentials for admin users	1	1
	Build timeline	Altiar to provide detailed timeline based on information provided in kick off meeting with roles for each step	1	1
	Design with ongoing feedback	Altiar to provide wireframe designs based for feedback and review from DfE stakeholders	2	4
	Implementation with ongoing feedback	Altiar to implement branded design and page structure with weekly updates for feedback and review from DfE stakeholders	4	9
	Historic data transfer	DfE to provide content in agreed format for import into the new platform by Altiar	9	10
	SSO integration	Work with DfE IT team to implement and test single sign on	4	7
	User acceptance testing	DfE stakeholders to review and feedback on site functionality / deliverables	10	11
	Site documentation and training guide	Altiar to provide tailored training guide for DfE users	12	12
	Super user training	Training sessions for administrators / super users	12	12
	User training	Arrange training sessions for general users (if required)	13	13

	Client sign off	DfE stakeholders to sign off overall implementation prior to launch	14	14
	Official launch	Release site and promotional materials to DfE users with support from Altiar	15	15
	Journal integration	The supplier will agree with the Contract Manager a plan to integrate the Department's existing journals subscription from [redacted] into the Research Evidence Directory. Timeline to be agreed during the contract term with the Contract Manager.	TBC	

Offboarding

The offboarding plan for this Call-Off Contract is:

From the date of termination of the contract Altiar will, within 30 days:

- Export any document files we hold in the original format named by the reference filename.
- Export all page content assets (text, images, videos, links) we hold in the original format.
- Export the following metadata in a human readable table-based format (excel, csv)
  - Projects
    - Ref ID
    - Title
    - Summary
  - Documents
    - Ref ID
    - Title
    - Summary
    - Published Date
    - Author name(s)
    - Source name(s)
    - Tag value(s)
    - Keywords
    - Read only flag
    - Archive flag

	• Filename ref • Uploader ref • Project refs • Groups • Ref ID • Name • Logo • Description • Users • Ref ID • Email • Role • Status • Group refs • Permissions • Ref ID • Document ref • Group refs • User refs • Transfer the above exports directly to the buyer via the preferred transfer method (email, OneDrive, FTP, mail, etc). • Undertake a one-off call with the buyer (if required). • Destroy all buyer data and backups held by us and evidence this where appropriate.
Collaboration agreement	N/A
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed **£1,000,000.** The annual total liability for Buyer Data Defaults will not exceed 125 **%**of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).

Insurance	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits [enter text].
Buyer's responsibilities	The Buyer is responsible for the following: (i) to make available its own representatives and its suppliers for meetings and promptly provide information, materials and documents reasonably requested by the Supplier from time to time. (ii) Where agreed, to provide office facilities, excluding car parking, at Buyer's address for Supplier's service delivery staff to perform the Ordered G-Cloud Services. (iii) to provide the proposed reporting timetable and report formats for governance and meetings; and (iv) to be responsible for communication to its organisation in respect of any agreed activity by the Supplier when undertaking services defined within this Call-Off Contract which may impact the Buyer's business.
Buyer's equipment	N/A

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners are as set out in the Service description and definition for Service ID: 77140531 8027 441.

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is BACS.
Payment profile	The payment profile for this Call-Off Contract is **monthly** in arrears. Licences will be paid up front, annually in advance and any other requirements will be paid monthly in arrears. The implementation fee will be paid in 3 monthly instalments and be paid in arrears as set out in Schedule 2.
Invoice details	The Supplier will issue electronic invoices **monthly** in arrears. The Buyer will pay the Supplier within **30** days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to CReD.Finance@education.gov.uk
Invoice information required	All invoices must include the Buyer's: • Purchase Order number; and • Change Authorisation Note number, as applicable.
Invoice frequency	Invoices will be sent to the Buyer monthly in arrears.
Call-Off Contract value	The total value of this Call-Off Contract is £257,000 excluding VAT.

Call-Off Contract charges	The breakdown of the Charges is as per the Suppliers Service offer in Service ID: 77140531 8027 441 and in Schedule 2 of this Call-Off Contract.

Additional Buyer terms

Performance of the Service and Deliverables	N/A
Guarantee	N/A
Warranties, representations	N/A
Supplemental requirements in addition to the Call-Off terms	N/A
Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Public Services Network (PSN)	The Public Services Network (PSN) is the government's secure network. If the G-Cloud Services are to be delivered over PSN this should be detailed here: n/a
Personal Data and Data Subjects	Annex 1 and Annex 2 of Schedule 7

1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.

2.2 The Buyer provided an Order Form for Services to the Supplier.

Signed	Supplier	Buyer
Name	[redacted]	[redacted]
Title	CEO	[redacted]
Signature	[redacted]	[redacted]
Date		

Schedule 1: Services

The Supplier will provide the Buyer with the services as outlined in G-Cloud Service offering with Service ID: 77140531 8027 441

Altiar is an easy-to-use mobile and web-based knowledge management platform. An efficient and powerful way to collate and distribute content, it allows users to locate the information they need, when they need it – without needing to know where it is held and who owns it.

Make your knowledge more customer focused
Altiar find the right insights to help you stay close to your customers and anticipate their needs. For a more dynamic, agile, and competitive business.

Make your knowledge more connected
Altiar makes it easy for everyone to stay connected. Use our customer insight platform to respond quickly to customer needs, and work smarter with your wider business, nationally and internationally.

Completely bespoke to you
Consulting with you, Altiar design and build your portal around your branding, your organisation, and your content needs.

Have expert help on hand
Altiar's responsive team of developers and designers can support yours seamlessly, whenever you require.

Tailor your teams
Altiar set custom permissions for different user groups and departments, all from a single source of content.

Find what you need fast
Reclaim wasted time and resource. Get your data to the people that need it with seamless integration, plus search and content notifications and custom-newsletters.

Discover which research adds value
Reveal which vendors produce the most useful research so you can commission more relevant reports or renegotiate pricing.

Track the impact
See who used which content, when, and understand how they added value.

Stay close to your customers
Find the right insights to make your knowledge more focused on your customers and anticipate their needs.

The RED system will act as a central place for DfE staff to search both the internal and external evidence base and to find information about research which is currently live (both internal and where possible, externally funded).

RED will act as a 'one stop shop' for information on research evidence services, as well as drawing together relevant research information. It will:

- Help users at every stage of the research process.
- Help upskill researchers.
- Provide alerts to new material that may be of interest, tailored to individual interests.
- Share learning and show-case good practice, ensuring best value for money from our efforts.

RED will allow users to quickly and easily:

- explore robust relevant research evidence.
- learn more about research, aiding coordination.
- help them identify genuine gaps in the evidence base and get help with filling them.
- build research skills (both for analysts and non-analysts).
- find details about relevant research associates and suppliers.

It will also help make better use of research and policy investment by:

- Making robust internal and external research evidence more accessible to improve policy decisions.
- Marshalling evidence to help DfE make more strategic decisions about the use of research resource.
- Improving coordination of research and analysis,
- Raising awareness of the research services offered within the department.
- Increasing compliance with government commitments on research and procurement processes.
- Promote methodological rigour, share learning, and show case good practice.

Altiar have regular client calls where Altiar receive updates on developments in the client business, review use of the platform, ways to improve engagement and potential design changes or functionality uses. This is to ensure continuing engagement of users and to maximise usage within the business. Working with dozens of clients over the last 10 years, working with Insight, Intelligence, Customer Experience and Analytics teams within those global brands provides Altiar with a deep understanding of the challenges faced by those teams and many different ways those challenges can be overcome.

Feedback Altiar receive from clients is fed into the development roadmap, progressed to new features, and made available to all users of the Altiar platform. This means that Altiar can share best practice, expertise and capabilities from working with global brands over years of partnership.

DfE Solution and Features

This would be a PaaS (Platform as a Service) solution, hosted, managed, and supported by Altiar utilising our Microsoft Azure cloud-based infrastructure.

The key elements and features of the DfE system would be:

- Specific named, fully branded portal with custom designed pages – the portal will look and feel totally on brand with all pages designed to ensure a visually appealing and user-friendly system resulting in maximum engagement with users.

- Fully customised structure for categorization.

- Intuitive navigation making it simple for users to find their way around the site to access the content they are looking for.

- Powerful search with machine learning. This includes all file metadata in addition to all file content of all file types.
- All formats and types of content will be included and categorised including all MS Office file types, PDF, video, voice, images, HTML, SSRS.
- No restrictions on file sizes.
- All content types are fully viewable directly from the portal but can also be downloaded or shared.
- Ability to group content into projects.
- User entry to the system via SSO automated login would make access to the portal seamless whilst also directing the user to the most relevant area of the site for their role.
- Custom designed and fully branded automated notifications and alerts which can be quickly set and customized by users and groups.
- Highlighted content on spotlight pages to promote content to users.
- Newsletter functionality for sending fully branded and customised newsletters to groups of users highlighting content and knowledge on a frequent basis directly from the portal.
- User Digest contains trending content and updates from your subscriptions.
- Ability for users to save searches and set frequency of notification of new results, upload to and share content directly from the site as well as view all interactions with the platform.
- Ability for third parties to access and upload to system if required.
- Potential to embed dashboards and charts from other applications.

  24/7 access with support.

The Services the Supplier must provide are in line with the G-Cloud Services, Call Off contract description, Table 1 and in accordance with the published service definition with Service offer ID: 7714 0531 8027 441.

The Buyer can request in writing a change to this Call-Off Contract if it is not a material change to the Framework Agreement/or this Call-off Contract as per Clause 32. The Buyer shall have the option, by giving written notice to the Supplier to vary the Contract and request additional functionality that is in scope of the requirements set out in the ordered G-Cloud Service offer ID: 7714 0531 8027 44. The Buyer reserves the right to request additional functionality as required as part of on-going development and completion of post release.

The Supplier will work with the Buyer to agree timelines for implementation and prioritise additional functionality and incurred costs by Contract Variation. The Contract, including any Variations, shall remain effective and unaltered except as amended by Variation.

Table 1

PORTAL: Access	All DfE staff will have access to the portal. The system will only be accessible internally (i.e. by DfE users).
PORTAL: Single sign on	Users will not be required to use any additional login credentials to use the portal
PORTAL: User centred	The portal will enable users to quickly find the kind of research information that they are looking for. (Provisional design has 5 main sections): • Explore Research Evidence • Find research associates or suppliers • Learn more about DfE Research • Build research evidence • Build research skills
PORTAL: Content	The portal will at first be populated with existing guidance but also allow for creation of new content within the portal
PORTAL: Visual	The portal will look modern, visually appealing, simple to navigate, (uncluttered without too many sections or lengthy text)
PORTAL: Access levels	Different users will have different access levels. There will be different access levels for different users.
PORTAL: Design	Admins will be able to make limited changes to how the portal looks by adding, amending or deleting portal pages, text and graphics etc without needing coding skills. The contractor will make more involved changes where required.
PORTAL: Updating links	The links in the portal will be automatically updated when they change, to avoid them breaking
RED ACCESS	All DfE staff will have access to the RED. Users should be able to access it both from the portal, but also using links in documents, sharepoint pages etc

RED FRONTAGE – Visual	The frontage will look modern, visually appealing and simple to navigate (not long lists of directories, folders, and documents)
RED CONTENT: Document formats	System will allow for a variety of document formats to be shared (most importantly PDFs, word documents, Powerpoint slide packs)
RED CONTENT - Automatic inclusion of relevant gov.uk content	The evidence directory will be automatically updated when new content is published on the DfE gov.uk research pages, or when existing content on the gov.uk research pages is updated.
RED CONTENT – Automatic inclusion of other reputable organisation's relevant content	The evidence directory will be automatically updated with new content published on relevant external content. This will include (but not limited to):  There will be scope to change the list of organisations as the landscape changes.
RED CONTENT – Collections	Material relating to the same subject will be linked within a collection, e.g. reports of a survey conducted in multiple years. This can be applied to how the results are displayed and searched.
RED USER – Uploading research evidence	The system will allow users to upload individual research evidence documents into the repository. This will be done by automatically pulling results from a DfE SharePoint repository,
RED CONTENT- Associate and supplier database(s)	The system will include information about research associates and suppliers. This will be uploaded as a fully searchable excel sheet.
RED USER- Tagging	Admin will be able to tag documents in RED using tick boxes. The metadata schema will during the implementation and users should only be able to add these agreed tags. The tags may need to be

	reviewed from time to time so that new tags could be added where necessary.
RED USER - Tagging	When documents are scraped, the system will also pull relevant meta data such as the date of the report. Admin users will have scope to change these details/attributes.
RED ADMIN - Tagging	Admins will have the ability to change, add to and remove tags including document author labels via a popup form
RED CONTENT – User upload duplicate alert	The system will automatically check whether a document being uploaded has the same title as another document already within RED and alert the user so that they can decide whether to cancel the upload.
RED CONTENT – adding new versions of existing documents	Users will be able to upload a document as a new version of an existing document on the system
RED CONTENT – Admin Duplicate alert	The system will automatically alert admins when a document is uploaded that has the same title as another document already within RED, so that the admin can review them and decide whether to delete, rename or replace the existing version on the system in cases where a revised version has been uploaded. This will include when the system automatically adds content from gov.uk (which could be the published version of a document already held)
RED USER + ADMINS – Evidence grading	Users will be able to grade/rate evidence for each document. The system will allow users to search and filter for a certain grade of evidence.
RED USER: VIEW	Users will be able to view information about a document, an abstract (or abstract-type summary of) the document, or the full document. Users will be able to increase or reduce the size of fonts for viewing the document.
SEARCH – Meta	All users will be able to interrogate the evidence repository based on search criteria. This should scrutinise all meta data (expected to include *tags and titles)*
SEARCH - Summaries	All users will be able to interrogate the evidence repository based on search criteria. This will

	scrutinise both meta data and *abstracts or summaries* within all research evidence formats.
SEARCH – Full text	All users will be able to interrogate the evidence repository based on search criteria. This will scrutinise full-text narrative within all research evidence formats as well as meta data and summaries.
SEARCH - Formats	Users will have several search options: a. through typing a query into a search box b. through a more advanced search box format (adding filters or conditions, including using Boolean operators, such as AND, OR, NOT and NEAR), or by clicking on “buttons” to help them navigate through the contents of the repository
SEARCH – Simultaneous search	Users will be able to search all RED content and Journal articles at the same time. Our journal access is currently provided by EBSCO but the provider could change in the future.
SEARCH – Filter scope	Users will be able to filter searches to cover just: • internal content, • content on gov.uk, • content on other reputable websites, • journal articles, or a combination of these.
SEARCH - Conditions	Users will be able to apply further conditions to narrow searches and return a more refined set of results. Each condition adds a clause to the search query that is created and run when you start the search. A condition is logically connected to the keyword query (specified in the keyword box) by a logical operator (c:c) that is similar in functionality to the AND operator. It should be possible to add conditions relating to: • Publication date • Author (s) • Subject • Other meta data e.g. document type, research type, geographic scope
SEARCH RESULTS – Display	Users will be able to change the overall view of their search results.
SEARCH RESULTS – Display	The system will give a quick overview of the full content for a particular search (a bit like a contents page but with more information), as well as

	the links for individual documents, to help users decide whether to apply further filters. This could include: • number of items in totality • number by publication year, • number of each type of document (using tags) – e.g. number of literature reviews. With scope to click on document year or types to get further details (titles/summaries/full text) of just those selected (effectively filtering searches further).
SEARCH RESULTS – Evidence grading	The system will display a simple graphical summary of Evidence Grading scores (e.g. star ratings) for the evidence that has been found. It will also be possible to filter both initially and subsequently e.g. if you get 50 studies, to then filter to only see studies with a particular score or rating.
BOOKMARK DOCUMENTS	Users will be able to bookmark documents within the system
USER FRIENDLY	The system will be easy to use, and should not necessitate user training, The supplier will provide a custom user guide as part of the implementation.
ACCESSIBILITY	The system will be accessible for staff who use adaptive technology (such as machine readers)
RED: BOOKMARKS	Users will be able to bookmark documents within the system
VIEW	Users will be able open a variety of content material in read only format. Including: Word, pdf, powerpoint
RED feedback: remove item request	Users will be able to feedback to the admin team if they think that a specific item in RED should be removed (whether because it duplicates other content, has been replaced with more up to date material, or because of quality concerns) eg. via email links to admin contacts

Admin	The admins will have full control of (initial) look and feel and changes can be made quickly.
MI collection – document, how many and when	The system will record the number and date of views for each document.
MI collection – document, who	The system will record the number of views for each document by subject area
MI collection – searches	The system records what searches users under-took
MI collection - content	The system records the number of documents on RED on each date (disaggregated for subject and against other meta data)
MI reports: Usage statistics reports	Admins will be able to get reports providing sta-tistics on usage of both the portal and RED, with filters to look at this for: • a specific time frame, • content source (e.g. gov.uk reports only) • by document keyword/tag Reports will include the number of searches, a tally of search terms, and how long searches are taking to return results (latter to monitor system responsivity).
MI reports: View number and date of hits	Users will be able to view data on the number of times any specified document has been viewed for a specified time frame.
PORTAL: Further information	The system will make it clear where to go to get further information where needed about the in-formation in the portal, e.g. on research pro-cesses (this will usually be sign posting to a team/division rather than an individual).
PORTAL: Internal expertise	The portal will provide information that helps us-ers find a relevant analyst, so that they can seek advice where needed.
RED: Signposting for externally owned content	Meta data for externally authored and owned content will give the original author's name as author and the name of the responsible organi-sation.
Security	The system will meet DfE security requirements

TECHNICAL SUPPORT - maintenance	There will be technical support for the system once it has been launched to ensure continued functioning (maintenance and fixing problems)
TECHNICAL SUPPORT – continuous development	There will be technical support to help iterate and improve the system after it has been launched
CONTINUITY: Export function	Any meta data, summaries or information stored on the system will be able to be exported and transferred out of RED and into another location (for example to enable us to move content to a different platform or package).
Response Time	Software Response Times for failure to meet 95% of all results links to be loaded in less than 8 seconds. Feedback during the delay is especially important if the response time is likely to be highly variable, since users will then not know what to expect
PORTAL welcome	Tailored landing page welcome for user, using their first name (e.g. “Welcome Al”),
PORTAL AND RED USER – NOTIFICATIONS	Users will be able to opt *into s*ubscribing to receive alerts or “push notifications” of new portal and/or RED content that they might be interested in. They should be able to specify the type of notifications that they would like (email, alert when they enter the system) and frequency. (“Push” technology, or server push, is a style of Internet-based communication where the request for a given transaction is initiated by the publisher or central server. It is contrasted with pull/get, where the request for the transmission of information is initiated by the receiver or client.)
PORTAL AND RED USER – TAILORING – PREVIOUS USE	The system will provide users who want them with notifications *tailored to their previous use of the system.* For example, if they search for a particular journal repeatedly they could be notified when a new volume is published.

PORTAL AND RED USER – TAILORING – INTERESTS	The system will allow users to get alerts based on their saved searches.
Tailoring – display	Users will be able to display details of the interests they have logged and the alerts they have opted into, and to edit whenever they choose to do so (including turning off).
Non-Functional Requirements – Disaster Recovery	Integrated into Enterprise Disaster recovery plan.
Non-Functional Requirements – Concurrent Users	Be able to cope with concurrent users.
Non-Functional Requirements – Load Testing	Be able to cope with maximum input at peak times.
Non-Functional Requirements – Audit	Be able to an Audit trail of a person or entity using the system.
Non-Functional Requirements – Back Up Policy	Conform to DoE backup policy.

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) cannot be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Quotation

All amounts quoted exclude VAT or applicable sales taxes.

Table 2 - Year 1 (not including additional fees)

Product/Service	**Cost (£)**	**Payment Terms**
Implementation fee	[redacted]	3 monthly instalments
Annual Licence fee	[redacted]	Annual in advance
Total	[redacted]	

Table 3 – Year 1 and Year 2 (not including additional fees)

Product/Service	**Cost (£)**	**Invoice due**
Annual Licence Fee	[redacted]	June 2021
Implementation Fee	[redacted]	July 2021
	[redacted]	August 2021
	[redacted]	September 2021
Year 1 Total	[redacted]	
Year 2 Total	[redacted]	
Overall Total for Year 1 and Year 2	**£257,000**	

No additional charges over and above the licence fees. The implementation fee and annual licence fees are inclusive of all work to cover the requirements of DfE and as set out in the Specification document.

The annual licence fees of £[redacted] are payable annually in advance and includes:

- [redacted] DfE users
- Access to all features of the platform
- Always upgraded to the latest platform version
- Fully managed hosting of the platform including data storage costs.
- All support for super users/admin users included.
- Management and amendment of all elements of the system throughout the year

Definition - Searchable Content - means any content indexed within the Software, no matter where it is stored;

If at any time whilst using the Software, the aggregated amount of Searchable Content indexed within the software exceeds [redacted] , the Customer and Supplier shall be obliged to agree:

a) to remove such content so as not to exceed the amount of Searchable Content; or

b) to agree by variation an increase in the amount of Searchable Content.

The implementation fee of [redacted] is to run for 15 weeks from contract commencement and will be paid in 3 instalments monthly in arrears as set out in Table 3.

Implementation fees include:

- Configuration of platform
- Uploading of historic content
- Design of fully branded custom pages
- Design of newsletters/notifications
- Integration of source feeds
- SSO implementation
- Custom user guide design
- Training for super users

Additional features

This is a guide price for additional features and development. Bespoke proposals will need to be scoped and costed per individual requirement to ensure the appropriate skill set and level of resource is accessed.

Table 4

Feature Development	**Small**	**Medium**	**Large**
Number of weeks delivery	1-2	4-8	10+
Day Rate	[redacted]	[redacted]	[redacted]
Development day	[redacted]	[redacted]	[redacted]
Costs	[redacted]	[redacted]	[redacted]

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)

- 8.59 to 8.60 (Data protection
- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'.
2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'.
2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services.

4.1.2 apply all due skill, care and diligence in faithfully performing those duties.

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer.

4.1.4 respond to any enquiries about the Services as soon as reasonably possible.

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer.

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents, or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party.

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on its own due diligence.

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract, it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there is an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it is not possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000.

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit.

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employer's liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement, or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers.

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances.

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance.

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended, or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly.
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer.

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity does not apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title, or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it cannot comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.5.1 rights granted to the Buyer under this Call-Off Contract

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.6.1 modify the relevant part of the Services without reducing its functionality or performance.

11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer.

11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer.

11.7 Clause 11.5 will not apply if the IPR Claim is from:

11.7.2 the use of data supplied by the Buyer which the Supplier is not required to verify under this Call-Off Contract

11.7.3 other material provided by the Buyer necessary for the Services.

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body.

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes.

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request.

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions.

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject.

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

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

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

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

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

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

13.6.6 buyer requirements in respect of AI ethical standards

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached, or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational, and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form, and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security, and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term

of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software, and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided.

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control.

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

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

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

16. Departmental Security Standards are outlined in Schedule 8.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee.

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided.

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses.

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied.

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so.

18.5.2 an Insolvency Event of the other Party happens.

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business.

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer does not pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who is not relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration.

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry.

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer.

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer.

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law.

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message.

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18-month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a

central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer.

21.6.2 there will be no adverse impact on service continuity.

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier.

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer.

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data.

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations.

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition.

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control.

22.1.2 other information reasonably requested by the Buyer.

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance

and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form.

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form.

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses, or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

25.1 If either Party uses the other Party’s premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer’s premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises.

25.5.2 comply with Buyer requirements for the conduct of personnel.

25.5.3 comply with any health and safety measures implemented by the Buyer.

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury.

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who is not Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform.
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits, and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably. requested by the Buyer.

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause.

29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer.

29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause, but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer does not have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it is not a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party cannot agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation or End this Call-Off Contract by giving 30 days' notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration Agreement – N/A

Schedule 4: Alternative clauses - N/A

Schedule 5: Guarantee - N/A

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: • owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes. • created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which is not available to the Supplier otherwise than under this Call-Off Contract but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.

Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but is not limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').

Control	'Control' as defined in section 1124 and 450 of the Corporation Tax. Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR

Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14-digit ESI reference number from the summary of the outcome screen of the ESI tool.

Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare. • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party is not reasonably available. The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure. • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into. • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).

Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trademarks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information. • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction. • all other rights having equivalent or similar effect in any country or jurisdiction

CIPS Renewal Receipt.msg

Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It is a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.

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.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.

Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity.
	• reward that person for improper performance of a relevant function or activity
	• commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and

	regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.

Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but is not limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier’s servants, agents, Suppliers and

	Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1: Processing Personal Data

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

1.1 The contact details of the Buyer's Data Protection Officer are: [redacted]
1.2 The contact details of the Supplier's Data Protection Officer are: [redacted]
1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
1.4 Any such further instructions shall be incorporated into this Annex.

Descriptions	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation,

	the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: The Supplier will be responsible for providing electronic access to a research portal that will provide a single place where DfE staff can search the department's external and internal evidence base. We will work with the chosen Supplier to ensure that any documents and information on the system cannot be altered and will be 'view only'. **The Supplier is Controller and the Buyer is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data: n/a **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● Business contact details of Supplier Personnel for which the Supplier is the Controller ● Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller
Duration of the Processing	Personal data (staff emails and names) will be kept for as long as the contract with the supplier is in place. Contract duration will be 2 years with an option to extend for a year.

	We will ensure that we have clauses in the contract which will specify that any personal data will be removed from the supplier's systems once the contract ends.
Nature and purposes of the Processing	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment Processing, statutory obligation, recruitment assessment etc] The main personal data being shared with the contractor will be staff's names and email addresses. This would be used to both enable single sign on and to personalise the service to allow users to create email alerts or personal reading lists. We expect that the data (staff names and work emails) will be drawn from the department's own records of DfE staff which will be updated on a regular basis to ensure that new staff have access to the system. This data will only be used for the purposes listed above and staff using the system will not be able to see personal data stored on the system. The only exception is we want to allow users to review documents on the system and we may choose to display who has left a review. We also may want to signpost users to the analytical teams who have produced a piece of research and therefore may display the name and work email of the team lead on the system so that users can get in touch with them if they want to find out more about the work.
Type of Personal Data	Names and staff email addresses. We expect this will be obtained via electronic transfer.
Categories of Data Subject	

	Dfe Staff
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	Personal data (staff emails and names) will be kept for as long as the contract with the Supplier is in place. Contract duration will be 2 years with an option to extend for a year. We will ensure that we have clauses in the contract which will specify that any personal data will be removed from the supplier's systems once the contract ends.

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 4 of the Framework Agreement (Where one Party is Controller and the other Party is Processor) and paragraphs 17-27 of Schedule 4 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the buyer

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

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

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR.

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

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

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

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every 6 months on:

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

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

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

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

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

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

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses

2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex.

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information.

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

(g) take all reasonable steps to ensure the reliability and integrity of any of its personnel who have access to the Personal Data and ensure that its personnel:

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

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

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

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

(i) nature of the data to be protected.
(ii) harm that might result from a Data Loss Event.
(iii) state of technological development; and
(iv) cost of implementing any measures.

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

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

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

3. Data Protection Breach

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

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

(b) all reasonable assistance, including:

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

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

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

and/or

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

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

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

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

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

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

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

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

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant central government body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant central government body.

7. Liabilities for Data Protection Breach

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

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

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

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing disputes).

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

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

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

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

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third-party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Not used

9. Termination

9.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (joint controller agreement), the Buyer shall be entitled to terminate the contract by issuing a termination notice to the Supplier in accordance with Clause 18.5 (Ending the contract).

10. Sub-Processing

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

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

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

11. Data Retention

11.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to

be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Schedule 8: Buyer Security

Annex 1: Departmental Security Standards

1. Departmental Security Standards for Business Services and ICT Contracts

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

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

“GSC” “GSCP”	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
“HMG”	means Her Majesty’s Government
“ICT”	means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
“ISO/IEC 27001” “ISO 27001”	is the International Standard for Information Security Management Systems Requirements
“ISO/IEC 27002” “ISO 27002”	is the International Standard describing the Code of Practice for Information Security Controls.
“ISO 22301”	is the International Standard describing for Business Continuity
“IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing”	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
“Need-to-Know”	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
“NCSC”	The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
“OFFICIAL” “OFFICIAL-SENSITIVE”	the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP). the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.
“RBAC” “Role Based Access Control”	means Role Based Access Control. A method of restricting a person’s or process’ access to information depending on the role or functions assigned to them.

“Storage Area Network” “SAN”	means an information storage system typically presenting block-based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
“Secure Sanitisation”	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hard-copy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
“Security and Information Risk Advisor” “CCP SIRA” “SIRA”	means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
“Senior Information Risk Owner” “SIRO”	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arm’s length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
“SPF” “HMG Security Policy Framework”	means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.17 Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

1.18 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.

1.19 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

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

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

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

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

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

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

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

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

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

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

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

Schedule 9 – Exit Plan

From the date of termination of the contract Altiar will, within 30 days:

- Export any document files we hold in the original format named by the reference filename.
- Export all page content assets (text, images, videos, links) we hold in the original format.
- Export the following metadata in a human readable table-based format (excel, csv)

  Projects

  - Ref ID
  - Title
  - Summary

  Documents

  - Ref ID
  - Title
  - Summary
  - Published Date
  - Author name(s)
  - Source name(s)
  - Tag value(s)
  - Keywords
  - Read only flag
  - Archive flag
  - Filename ref
  - Uploader ref
  - Project refs

  Groups

  - Ref ID
  - Name
  - Logo
  - Description

  Users

  - Ref ID
  - Email
  - Role
  - Status
  - Group Refs

  Permission

  - Ref ID
  - Document ref

    - Group refs
    - User refs

- Transfer the above exports directly to the buyer via the preferred transfer method (email, OneDrive, FTP, mail, etc).
- Undertake a one-off call with the buyer (if required).
- Destroy all buyer data and backups held by us and evidence this where appropriate.