Crown Commercial Service

RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated 02/09/2022 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm1234. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.
13. Annex 2 – Ethical Walls Agreement

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

.1.1 the Framework, except Framework Schedule 18 (Tender);

.1.2 the Order Form;

.1.3 the Call Off Terms; and

Crown Commercial Service

.1.4 Framework Schedule 18 (Tender).

Section A
General information

Contract Details	
Contract Reference:	con_17461
Contract Title:	Data Science Services – Oracle Intelligent Advisor
Contract Description:	Procurement of a full range of specialised services for the implementation of Oracle's Intelligent Advisor (IA) and associated technologies and applications, including Oracle CX, Oracle Service Cloud, Siebel, SOA and Oracle EBS.
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	Maximum of £2,851,089 ex VAT
Estimated Year 1 Charges:	£1,425,599 ex VAT
Commencement Date: this should be the date of the last signature on Section E of this Order Form	12/12/2022

Buyer details
Buyer organisation name Department for Education
Billing address Your organisation's billing address - please ensure you include a postcode Accounts Payable, ASC Purchasing, Cheylesmore House, Quinton Road, Coventry, CV1SWT

Crown Commercial Service

Buyer representative name
The name of your point of contact for this Order
[REDACTED]

Buyer representative contact details
Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.
[REDACTED]
[REDACTED]

Buyer Project Reference
Please provide the customer project reference number.
Proj_7007

Supplier details

Supplier name
The supplier organisation name, as it appears in the Framework Agreement
Bramble Hub Limited

Supplier address
Supplier's registered address
9e Albert Embankment, London, SE1 7SP

Supplier representative name
The name of the Supplier point of contact for this Order
[REDACTED]

Supplier representative contact details
Email and telephone contact details of the supplier's representative. This must include an email for the purpose of Clause 50.6 of the Contract.
contact@bramblehub.co.uk

Order reference number or the Supplier's Catalogue Service Offer Reference Number
A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number.
[REDACTED]

Guarantor details

Crown Commercial Service

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Guarantor Company Name
The guarantor organisation name

Not Applicable

Guarantor Company Number
Guarantor's registered company number

Not Applicable

Guarantor Registered Address
Guarantor's registered address

Not Applicable

Crown Commercial Service

Section B
Part A – Framework Lot

Framework Lot under which this Order is being placed
Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.

1. TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2. TRANSITION & TRANSFORMATION	☐
3. OPERATIONAL SERVICES	
a: End User Services	☐
b: Operational Management	☐
c: Technical Management	☐
d: Application and Data Management	X
5. SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
See above in Section A

Contract Period
Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:

Crown Commercial Service

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)
3	60 (5)
5	60 (5)

Initial Term Months
24 Months

Extension Period (Optional) Months
12 Months

Minimum Notice Period for exercise of Termination Without Cause 30 Days
(Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)*

Sites for the provision of the Services
Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.

The Supplier shall provide the Services from the following Sites**:**
Buyer Premises:

Cheylesmore House,
5 Quinton Road,
Coventry,
CV1 2WT.

Services will be delivered using a blended approach between on-site & remote working. Each Statement of Work (SOW) will define the working arrangements.

Supplier Premises:

Not applicable

Third Party Premises:

Not Applicable

Buyer Assets
Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms
Full list of assets to be confirmed.

Additional Standards
Guidance *Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.*

Not Applicable

Crown Commercial Service

Buyer Security Policy
Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.


Security_Clauses.docx

Buyer ICT Policy
Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.


security-policies-brochure.pdf

Insurance
Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.

Third Party Public Liability Insurance (£) – Not Applicable (same as default)

Professional Indemnity Insurance (£) – Not Applicable (same as default)

Buyer Responsibilities
Guidance Note: list any applicable Buyer Responsibilities below.

The Authority is responsible for providing timely access to all sites and personnel relating to the delivery of the service

In respect of this Contract, the Buyer, as project owner, will perform the role, responsibilities, obligations and duties expressed to be on the Buyer's part in the Statement of Work within the relevant specified timescales specified in the Statement of Work or, if none, as soon as reasonably possible.

Goods
Guidance Note: list any Goods and their prices.

Not Applicable

Crown Commercial Service

Governance – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	X
Part B – Long Form Governance Schedule	☐

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	X
Part B – Long Form Change Control Schedule	☐

The Part selected above shall apply this Contract.

-

Section C

Crown Commercial Service

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses *(see Annex 3 of Framework Schedule 4)*
This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules
Guidance Note: Tick any applicable boxes below

Additional Schedules	Tick as applicable
S1: Implementation Plan	X
S2: Testing Procedures	X
S3: Security Requirements (either Part A or Part B)	Part A
S4: Staff Transfer	X
S5: Benchmarking	X
S6: Business Continuity and Disaster Recovery	x
S7: Continuous Improvement	X
S8: Guarantee	Not Applicable
S9: MOD Terms	Not Applicable

Part B – Additional Clauses
Guidance Note: Tick any applicable boxes below

Additional Clauses	Tick as applicable
C1: Relevant Convictions	X
C2: Security Measures	X
C3: Collaboration Agreement	Not Applicable

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses
Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	Not Applicable
Northern Ireland Law	Not Applicable
Joint Controller Clauses	Not Applicable

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Crown Commercial Service

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)
Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.

Not Applicable

Additional Schedule S4 (Staff Transfer)
Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.

Part C shall apply at commencement of the Services and Part E shall apply on the expiry or termination of the Services or any part of the Services.

Additional Clause C1 (Relevant Convictions)
Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.

1.1 All supplier staff working on services in relation to this contract will need to undertake as a minimum, a BPSS security check.
1.2 The Supplier shall ensure that no Supplier Staff who discloses that they have a Relevant Conviction, or who is found to have any Relevant Convictions (whether as a result of a police check or through the vetting procedure of HMG Baseline Personnel Security Standard or through the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Services without the prior written approval of the Buyer. Subject to the Data Protection Legislation, the Supplier shall disclose the results of their vetting process, promptly to the Buyer. The decision as to whether any of the Supplier's Staff are allowed to perform activities in relation to the Call Off Contract, is entirely at the Buyer's sole discretion, acting reasonably.
1.3 The Supplier shall be required to undertake annual periodic checks during the Call Off Contract Period of its Staff, in accordance with HMG Baseline Personnel Framework so as to determine the Supplier Staff suitability to continue to provide Services under the Call Off Contract. The Supplier shall ensure that any Supplier Staff who discloses a Relevant Conviction (either spent or unspent), or is found by the Supplier to have a Relevant Conviction through standard national vetting procedures or otherwise, is promptly disclosed to the Buyer. The Supplier shall ensure that the individual staff member promptly ceases all activity in relation to the Call Off Contract, until the Buyer has reviewed the case, on an individual basis, and has made a final decision.
1.4Where the Buyer decides that a Supplier Staff should be removed from performing activities, as a result of obtaining information referred to in clauses 1.3 and 1.4 above, in relation to the Call Off Contract, the Supplier shall promptly and diligently replace any individual identified.

Crown Commercial Service

The Supplier shall ensure that any replacement staff will meet the provision set out in clause 11.1.2 of the call off terms."
• Please refer to the defined terms section for further information on 'Conviction' & 'Relevant Conviction'.
Conviction: Means other than for minor road traffic offences, any previous or pending prosecutions, convictions, cautions and binding over orders (including any spent convictions as contemplated by section 1(1) of the Rehabilitation of Offenders Act 1974 by virtue of the exemptions specified in Part II of Schedule 1 of the Rehabilitation of Offenders Act 1974 (Exemptions) Order 1975 (SI 1975/1023) or any replacement or amendment to that Order
Relevant Conviction: Means a Conviction that is relevant to the nature of the

Additional Clause C3 (Collaboration Agreement)
Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.

Not Applicable

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

Not applicable

Section D
Supplier Response

Commercially Sensitive information
Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

Successful supplier responses are as found in the Department for Education's e-procurement system "Jaggaer", and are located in the Jaggaer record Proj_7007, ITT_1604.

Crown
Commercial
Service

Crown Commercial Service

Section E
Contract Award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

Name	**Neil Simpson**
Job role/title	**Director**
Signature	[REDACTED]
Date	**08/12/2022**

For and on behalf of the Buyer

Name	**Alex Botten**
Job role/title	**Commercial Category Lead**
Signature	[REDACTED]
Date	**09/12/2022**

Crown Commercial Service

Attachment 1 – Services Specification

APPENDIX B – SPECIFICATION

BACKGROUND TO THE CONTRACTING AUTHORITY

16.1.1 The DfE is a central government ministerial department, and the Education and Skills Agency (ESFA) is one of the executive agencies sponsored by the Department for Education. It is responsible for education, children's social services, higher and further education policy, apprenticeships and wider skills in England, and equalities. We work to achieve a highly educated society in which opportunity is equal for all, no matter your background or family circumstances.

16.1.2 The ESFA is accountable for £59 billion of funding for the education and training sector, providing assurance that public funds are properly spent, achieving value for money for the taxpayer, and delivering the policies and priorities set by the Secretary of State. It regulates academies, further education and sixth form colleges, and training providers, intervening where there is risk of failure or where there is evidence of mismanagement of public funds.

16.1.3 Data Science and Data Solutions are a fast-paced data services providing functions that cover data capture, data operations, governance, visualisation and analytics. Supporting funding, payments, performance monitoring and policy development for both DfE and ESFA. This particular contract is to support the function that delivers online forms and rule bases to meet business needs, developing complex validation rules or funding calculations, business requirements using an array of digital tools to progress project delivery.

17 BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

17.1.1 The Data Science division is responsible for a number digital services that support the ESFA such as Submit Learner Data (SLD) and online forms such as a suite of College Financial forms, Related Party Transaction (RPT) and Senior Mental Health (SMHL)

17.1.2 The Data Solutions divisions is responsible for a number of digital services that support the DfE such as a suite of T-Levels forms and Educational Setting Status as well as a Change & Release management function.

17.1.2 All services are was built using strict agile principles and it is maintained and enhanced using a principle of continuous improvement managed through a Kanban approach.

17.1.3 All services are built with security and user needs in mind. All services use an approved DfE authentication service such as Identity and Management Service (IdAMS) or DfE sign in (DSI) They comply with GDS standards as well as accessibility standards. Users can be both internal and external depending on the service.

17.1.4 The current team has a typical skill mix of Developers (Intelligent Advisor (IA), Java, Javascript, .Net and C#, Microsoft Azure, Weblogic, Microsoft O365 Sharepoint skillsets), Testers, Business Analyst, Change & Release Manager and a Delivery Manager. There is a shared DevOps function which assists in management of the infrastructure and environment.

17.1.6 Primary location will be ESFA Cheylesmore House, Coventry. Very occasionally travel may be required to the DfE/ESFA sites in London or across England where required.

17.1.7 There will be a requirement for work patterns to be office based up to 3 days a week based on business need as agreed with the Head of Digital Data Solutions (DDS). Remote meetings will be held using Microsoft Teams.

18. SCOPE OF REQUIREMENT

18.1.1 A service is required to manage and implement changes for Data Science and Data Solutions in order to support the business need, maintain continuous improvement, fix issues and enhance it to meet the agreed requirements of other funding systems.

18.1.2 The new service will need to undertake a knowledge transfer (KT) exercise with the existing managed service. This will need to be complete by 17th DECEMBER 2022 when that service ceases. It is a requirement that this KT exercise incorporates the creation of any necessary documentation (saved in a central area) or knowledge artefacts needed to build the understanding of these services and how they are maintained, enhanced and operated.

18.1.3 The service required is from October 2022 until 9th October 2024 with an option to extend for a further year, and the business hours will be Monday – Friday 9am-5pm. The maximum value for the contract is up to £2.8m [Ex VAT] and we would expect the core team to be made up of the following roles:

- IA Developers/Dev Ops (Lead, Senior and Standard)
- Change and Release Manager

18.1.5 Any changes needed by Data Science or Data Solutions as a result of priorities directed by the Product Manager should be clearly documented in user stories in the backlog and in process documentation. The resultant code should adhere to any relevant coding standards and architecture should be documented to reflect the work carried out and any reflect any changes to the overall solution.

18.1.6 The approach to development and support should follow agile principles appropriate to the need in question (e.g., scrum, Kanban). It is expected this would be supported by necessary agile ceremonies.

The technologies in use are:

Crown Commercial Service

19

General overview of system	• Azure instances of RHEL 8.1 • Running Oracle Weblogic 14 in a resilient cluster • Running Intelligent Advisor in Weblogic • Integration with third party authentication systems using both SAML and OIDC • Azure SQL for data storage and processing • .NET core applications for integration • Java applications for integration • Javascript and web technologies
Main framework	Oracle's Intelligent Advisor (IA)
Main code/language	.NET, .NET Core, #C, Java, JavaScript
Any other code /languages/frameworks	T SQL, Blazor
Any other components	Integration to Microsoft Sharepoint O365 (record creation and document storage only)
Data storage	Azure SQL, Azure storage accounts (Tables), Classic Storage accounts for backups
Hosting platform	Azure and Redhat Linux servers
Hosting type	PaaS (Backend services)
Version control system and repo	Azure GIT
Build & Release	Azure DevOps pipelines and Weblogic console deployment
Integration components	Bespoke integration written in Java and .NET running on Redhat
Development environment	Azure VMs, DfE laptops
Testing tools	.Net automation framework, Sortsite, JAWs, Dragon
Telemetry/logging tools	Weblogic inbuilt login

THE REQUIREMENT

19.1.1 The supplier must be able to deliver outcomes utilising the following skills to be able to maintain and run the Data Science and Data Solutions services:

- Expert in-depth knowledge of Intelligent Advisor both from the perspective of rule writing and integration
- Expert in-depth knowledge of Weblogic 14
- Excellent knowledge of programming languages such as Java, C#, HTML, JavaScript/CSS
- Back-end storage technologies such as SQL server

- Knowledge of PaaS environments
- Able to successfully develop software using modern engineering practices such as Test-Driven Development and Continuous Integration & Deployment in an Azure DevOps environment
- Non-Functional testing with the ability to analyse & communicate the test outcomes relating to recoverability, resilience, performance and scalability.
- Knowledge of GDS Standards, Technology Code of Practice or equivalent, using open distributed version control systems such as GitHub
- Able to design, develop, and maintain RESTful APIs
- Able to design, develop and maintain SOAP APIs
- Knowledge of IT Health Checks, penetration tests and implementation of remedial plans
- Knowledge of change and release management software development lifecycle ITIL methodologies

19.1.2 The supplier will have a proven track record in delivering secure digital services by applying NCSC cyber security principles and industry standard protocols

19.1.3 The Supplier will:

- Deliver their services in accordance with DfE's Departmental Security Standards and Special Clauses for Contracts.
- Support the requirement to flex by the teams up or down over the course of the contract and in line with the business needs.
- Manage their resources to show "value for money" by ensuring that all roles are fulfilled adequately and have been fully utilised within the SOW
- Ensure that there are sufficient resources in place to meet the business's need to "keep the lights on"

19.1.4 The Supplier will ensure all staff are as a minimum BPSS checked, with all supplier staff working on the contract to be minimum enhanced BPSS immediately and SC clearance may be required. We reserve the right to bring this in on a Statement of Work basis.

19.1.4 The supplier must be able to work collaboratively with other digital and technology service providers in a blended team environment.

Crown Commercial Service

20 KNOWLEDGE TRANSFER

20.1.1 The Supplier shall:

- Ensure that all work delivered within the Statement of Work (SoW) has been fully documented and saved in an agreed central location.
- Support knowledge transfer to enable the Data Science and Data Solutions services to increase the number of permanent civil servants in digital roles.
- The Supplier shall develop and maintain documentation within the customers document repositories (e.g., Azure Wikki, SharePoint etc.) that describe all the systems and procedures used to provide services to the Customer.
- The Service Provider is to deliver a full copy of the system documentation within 5 working days of being requested to do so by the Customer.

21 GOVERNANCE

21.1.1 The Supplier shall comply with the Customer's governance and operation model, as may be updated from time to time, including arrangements for:

- Contract and Supplier Management
- Service Management
- Portfolio, Programme and Project Management
- Strategy and Enterprise Architecture

21.1.2 The Supplier will need to appoint a Service lead who shall:

- be contactable by the Customer during normal working hours
- attend regular Customer meetings at locations and frequencies specified by the Customer.
- attend ad-hoc meetings with the Customer when requested to do so.
- The Supplier shall identify a Senior Manager/account manager to be the point of escalation for any issues that cannot be resolved by the Service lead.
- The Service Provider shall not replace the Service Manager or the Senior Manager during the contract without the Customer's prior written agreement to the proposed replacements, such consent not to be unreasonably withheld. For the avoidance of doubt this will exclude any changes caused by the relevant employee of the service supplier leaving the employment of the supplier for any reason.

- The Supplier shall prepare and maintain a Risk Register identifying all risks to the support and operation of the Services.
- The Supplier shall prepare and maintain an Issue Register identifying all issues relating to the support and operation of the Services.
- Deliver the roadmap as per prioritisation as directed by the Product Manager

22. KEY MILESTONES AND DELIVERABLES

22.1.1 The following Contract milestones/deliverables shall apply:

This contract seeks to enable the Data Science and Data Solutions services to continue to operate successfully enabling it to deliver the necessary business-as-usual (BAU) work and any enhancements the business requires.

It will also allow technical improvements to be carried out to maintain currency within an ever-evolving technology landscape as falling behind in adopting current software versions or innovative approaches becomes costly to rectify if done retrospectively.

Business As Usual (BAU) is a business requirement function which must be met yearly for the services to continue to operate and function:

- Support any existing services
- Support any new live services
- Support change & release project go-live and existing change & release service activities (Data Solutions only)

23. MANAGEMENT INFORMATION/REPORTING

23.1.1 The Service Provider shall provide a written monthly report which provides the information required by the Customer to assess the quality of the services provided and to determine the payment due for the services as detailed in the contract.

23.1.2 As a starting point the report shall include the detail below, but this may iterate over time to meet user needs.

- an executive summary
- details of performance against all agreed KPIs

- an explanation of the reasons for any failure to achieve target performance levels, together with description of any steps being taken to avoid any problems recurring
- details of any planned enhancements or maintenance and the way in which any consequent service disruption will be minimised
- details of any successfully implemented enhancements
- details of Service downtimes in relation to enhancements, maintenance or upgrades and the implications for service availability
- details of the current technology roadmap showing expected technology changes and opportunities for the Customer for the next 6 months
- a summary of the risks and issues register, identifying the priority risks/issues of the operation of the services
- All reports are to be provided by the Service Provider electronically in a format that can be read by the Customer 3 working days ahead of the monthly checkpoint meetings.
- The Service Manager, and other Service Provider staff as deemed appropriate by the Customer, shall attend Monthly Review Meetings, as detailed in the contract.

24. EXIT MANAGEMENT

24.1.1 The Supplier shall be required to work closely with the Authority to support the exit and transition from the contract including support for new services and the transfer of operational knowledge.

24.1.2 The Supplier shall provide a dedicated exit manager to deliver the exit transition plan and deliverables therein.

24.1.3 The Supplier shall provide an exit transition plan no less than 3 months before contract end that will include but not limited to;

- A timetable of events
- Resources
- Assumptions
- Activities
- Responsibilities
- Risks

Crown Commercial Service

25. CONTINUOUS IMPROVEMENT

Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

26. QUALITY

26.1.1. Staff are expected to adhere to the Service team's coding standards, and quality assurance frameworks. The relevant standards for each project or team will be specified within Statements of Work (as these may vary from team to team) but may include frameworks such as the Government Digital Service (GDS) standards.

26.1.2. Staff are also expected to work to the Authority's security framework and policies.

26.1.3. The Potential Provider must demonstrate that their services adhere to quality management standards.

27. NOT USED

28. STAFF AND CUSTOMER SERVICE

28.1.1. The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

28.1.2. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract to consistently deliver a quality service.

28.1.3 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

28.1.4. If the Authority deems the Supplier to be providing poor performance the Authority reserves the right to terminate associated contracts early as per standard contract terms and conditions for RM6100: Technology Services 3.

29. SERVICE LEVELS AND PERFORMANCE – FULL LIST BROKEN DOWN IN "ATTACHMENT 4 SERVICE LEVELS"

The Authority will measure the quality of the Supplier's delivery and all support services must be provided in-line with the Authority's **Operational-Level Agreement (OLA):**

a. On-site or off-site support five (5) days a week at the Authority's offices in Coventry or other location as agreed with the Authority.
b. Service availability target for supported services is 99.5%.
c. Hours of service: Typically, 08:00 to 18:00 Monday to Friday, excluding English Bank holidays. In the event of a P1 or P2 incident by exception, out of hours support to be provided up until 22.00 and at weekends where required, not expected to be more than twice a year.
d. Incoming incidents and requests will be prioritised based on impact and the service provider will support the Authority in meeting the following SLAs:

Priority	Description and examples
Priority 1 (P1) - major incident	• Application unavailable to all users • Majority of application transactions are failing • Failure of critical application function • Business process failed for critical deadline due today • Widespread corruption of critical data • Failed business event, public reputation at risk
Priority 2 (P2) - significant	• Application working at less than 50% efficiency • > no of users • > intermittency • Less than 50% of application transactions are failing • Failure of important application function • Business process failed for critical deadline due within next two days • Significant corruption of data
Priority 3 (P3) - minimal	• Advice and guidance • Business process failed for non-critical deadline • Corruption of non-critical data
Priority 4 (P4) - negligible	• Non-impacting Incident • Advice and guidance • Business process failed for non-critical deadline • Corruption of non-critical data

30. SECURITY AND CONFIDENTIALITY REQUIREMENTS

The successful supplier will deliver their services in accordance with DfE's Departmental Security Standards and Special Clauses for Contracts.

We reserve the right to amend the security requirements based on the recommendations from the DfE security team.

DfE Security Standards detailed in Annex 1 Part C

Crown Commercial Service

31. PAYMENT AND INVOICING

Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

The Authority will provide a purchase order for each Statement of Work (SoW) Invoicing and payment will be monthly in arrears as per the Department's standard process.

Payment will be made monthly in arrears.

All invoices must include:

- Invoice number
- Purchase order number
- Statement of Work Reference
- A breakdown of Supplier Charges by:
- Any relevant milestone payment due
- Supplier Staff days
- Relevant rate payable

32. CONTRACT MANAGEMENT

32.1.1 Attendance at Contract Review meetings shall be at the Supplier's own expense.

32.1.2 The Supplier will need to appoint a Service lead who shall:

- be contactable by the Customer during normal working hours
- attend regular Customer meetings at locations and frequencies specified by the Customer.
- attend ad-hoc meetings with the Customer when requested to do so.
- The Supplier shall identify a Senior Manager/account manager to be the point of escalation for any issues that cannot be resolved by the Service lead.

- The Service Provider shall not replace the Service Manager or the Senior Manager during the contract without the Customer's prior written agreement to the proposed replacements, such consent not to be unreasonably withheld. For the avoidance of doubt this will exclude any changes caused by the relevant employee of the service supplier leaving the employment of the supplier for any reason.

- The Supplier shall prepare and maintain a Risk Register identifying all risks to the support and operation of the Services.

- The Supplier shall prepare and maintain an Issue Register identifying all issues relating to the support and operation of the Services.

- It is expected that Statements of Work (SoW) are responded to within 5 working days. The Supplier accepts 100% delivery of key milestones as set out in each Statement of Work.

33. LOCATION

33.1.1 **The primary location will be Department of Education (DfE), Cheylesmore House, Coventry. Very occasionally travel may be required to the DfE/ESFA sites in London or across England, where required.**

33.1.2 **There will be a requirement for work patterns to be office based up to 3 days a week based on business need as agreed with the Head of Digital Data Solutions (DDS). Remote meetings will be held using Microsoft Teams.**

The primary location of the Services will be carried out at Cheylesmore House, Quinton Road, Coventry, CV1 2WT.

33.1.4 Whilst the primary site is Coventry, and ideally supplier resources would be within reasonable commuting distance from Coventry, this does not preclude services being delivered remotely from supplier sites, from home or from other DfE sites by agreement. If the supplier encounters difficulties supplying resources to the primary site, to support team collaboration, the supplier would be encouraged to locate resources in a 'secondary' DfE site, to be determined by the department, applicable to the availability of resource.

The DfE reserves the right to request staff to come into the office as and when required for work packages deemed inside scope of IR35.

Examples of Authority locations below:

- Cheylesmore House, Quinton Road, Coventry, CV1 2WT
- 2 St Paul's Place, 125 Norfolk Street, Sheffield, S1 2FJ
- Sanctuary Buildings, Great Smith Street, London, SW1P 3BT
- Piccadilly Gate, Store Street, Manchester, M1 2WD

Crown Commercial Service

Overseas working is not permitted. We will not be looking to off-shore or near-shore this requirement.

Travel to the primary site will not attract expenses. Occasional travel may be required to DfE sites across England, travel to these sites must comply with DfE Travel and Subsistence policy.

Crown Commercial Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments [N/A]

#	Milestone Description	Milestone Payment amount (£GBP)	Milestone Date	Delay Payments (where Milestone) (£GBP per day)
M1	*[insert description]*	*[insert amount]*	*[insert date as per Outline Implementation Plan]*	*[insert amount]*
M2				
M3				
M4				
M5				

Part B – Service Charges [N/A – costings to be provided at Statement of Work level]

Charge Number	Service Charges
[Service Line 1]	
[e.g. SL1C1]	
[Service Line 2]	
[e.g. SL2C1]	

Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges

Job Area
Standard

IA Developers/DevOps .	[REDACTED]
Senior	
IA Developer/Dev Ops	[REDACTED]
Change & Release Manager	[REDACTED]
Lead	
IA Developer/Dev Ops	[REDACTED]

Payment

The payment profile for this Call-Off Contract is monthly in arrears. Other pricing and payment methods or a combination of pricing and payment methods to be agreed on each Statement of Work.

Call-Off Contract charge

For the maximum defined call-off period for this contract, the rate card will not be subject to review for the purposes of aligning with indexation.

Invoicing

Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

The Authority will provide a purchase order for each Statement of Work (SoW) Invoicing and payment will be monthly in arrears as per the Department's standard process.

Payment will be made monthly in arrears.

All invoices must include:
- Invoice number

- Purchase order number
- Statement of Work Reference
- A breakdown of Supplier Charges by:
- Any relevant milestone payment due
- Supplier Staff days
- Relevant rate payable

Travel and Subsistence

Detailed in Annex 1 part B "Commercial Policy Guidance – Supplier Expenses: Travel and Subsistence"

Crown Commercial Service

Part D – Risk Register

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8	Column 9	Column 10	Column 12
Risk Number	**Risk Name**	**Description of risk**	**Timing**	**Likelihood**	**Impact (£)**	**Impact (description)**	**Mitigation (description)**	**Cost of mitigation**	**Post-mitigation impact (£)**	**Owner**

Part E – Early Termination Fee(s)

Section Not Applicable. The Buyer retains the right to terminate without cause where no such calculation details are expressly set out in Attachment 2 (Charges) of the Order Form.

Attachment 3 – Outline Implementation Plan

[To be Agreed as part of each Statement of Work]

#	Milestone	Deliverables (*bulleted list showing all Deliverables (and associated tasks) required for each Milestone*)	Duration (*Working Days*)	Milestone Date
M1	[Concept Design]	[Statement of Requirements System/Application Specifications Interface Specifications Systems Testing Strategy Implementation Strategy and Plan Risk and Issues Management Plan		

		Outline Disaster Recovery Plan Project Schedule Service Management Plan]		
M2	[Full Development]	[Design Verification Reports Design Validation Reports Change Management Plan System/Application Implementation Plan Risk and Issues Management Project Schedule Service Management Plan]		
M3	[System User Testing]	[System Test Report Risk and Issues Management Plan Project Schedule Service Management Plan Defects Log Final Inspection and Testing Report]		
M4	[User Readiness for Service]	[Training Plan Risk and Issues Log Implementation Plan Operations Plan Data Conversion & Cutover Plan Project Schedule Service Management Plan]		
M5	[Implementation]	[Implementation Plan Training Scripts]		
M6	[In Service Support]	[Post Implementation Report Data Conversion and Cut-Over Plan Service Delivery Reports Risk and Issues Log Service Management Plan Defects Log]		

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

The Authority reserves the right to review on a quarterly basis that the service level monitoring process is robust and effective, and will also work with the supplier to make sure the measures to the service levels are reasonable and proportionate. Changes made will be communicated and agreed via Contract Variation.

The Supplier must demonstrate clear efforts to improve performance and commitment to achieving the agreed targets.

Repeated failure to meet the service level threshold may lead to further action being taken in line with the contract terms and conditions.

The Department reserves the right to amend the service levels and where applicable introduce service credits across the contract duration.

The Authority will measure the quality of the Supplier's delivery and all support services must be provided in-line with the Authority's Operational-Level Agreement (OLA):

e. On-site or off-site support five (5) days a week at the Authority's offices in Coventry or other location as agreed with the Authority.
f. Service availability target for supported services is 99.5%.
g. Hours of service: Typically, 08:00 to 18:00 Monday to Friday, excluding English Bank holidays. In the event of a P1 or P2 incident by exception, out of hours support to be provided up until 22.00 ~~,~~and at weekends where required, not expected to be more than twice a year.
h. Incoming incidents and requests will be prioritised based on impact and the service provider will support the Authority in meeting the following SLAs:

Priority	Description and examples
Priority 1 (P1) - major incident	• Application unavailable to all users • Majority of application transactions are failing • Failure of critical application function • Business process failed for critical deadline due today • Widespread corruption of critical data • Failed business event, public reputation at risk
Priority 2 (P2) - significant	• Application working at less than 50% efficiency • > no of users • > intermittency • Less than 50% of application transactions are failing • Failure of important application function • Business process failed for critical deadline due within next two days • Significant corruption of data
Priority 3 (P3) - minimal	• Advice and guidance

	• Business process failed for non-critical deadline • Corruption of non-critical data
Priority 4 (P4) - negligible	• Non-impacting Incident • Advice and guidance • Business process failed for non-critical deadline • Corruption of non-critical data

Service Levels and Rectification Measures

Service Levels				**Rectification Measures**
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
Service Timeliness	The Supplier shall successfully commence the services detailed in each Statement of Work within the required time period required by the Statement of Work 'Services' are defined as the individuals who will be performing services in relation to the agreed statement of work	**Good** – Per each SoW, services delivery starts on the date agreed in the Statement of Work. Tolerance of up to 5 days delay for accepted or exceptional circumstances, as agreed in advance with contract manager: **Approaching Target** – At least 90% SoWs issued up to the date of the most recent performance review have had their services commence within the required time period, as per the date specified within each SoW. Delays to commencement of services delivery have not exceeded 5 working days, for circumstances reasonably determined to be within the supplier's control. **Requires Improvement** At least 80% SoWs issued up to the date of the most recent performance review have had their services commence	The service level measure is **'Good'** across a 3-month period.	Rectification Plan Process pursuant to Clause 31 is followed.

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
		within the required time period. Delays to commencement of services delivery have exceeded 5 working days at least once, for circumstances reasonably determined to be within the supplier's control. Up to the date of the most recent performance review, at least one SoW has had services delayed by at least 10 working days for circumstances reasonably determined to be within the supplier's control **Inadequate** – Less than 80% of SoWs issued up to the date of the most recent performance review have had their services commence within the required time period, as per the date specified within each SoW - with delays caused by circumstances reasonably determined to be within the supplier's control. Or: Up to the date of the most recent performance review, at least two SoWs have had their services delayed by at least 10 working days for circumstances reasonably determined to be within the supplier's control.		

Crown Commercial Service

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
Statement of Work Response Rate	SOW's successfully responded to by the Supplier within 5 working days of receipt. 'Successfully' is defined as all relevant sections in the SOW being fully completed by the supplier and sent back to the Buyer within 5 working days of SoW being issued.	Good – 100% successful response rate for each SOW issued up to the date of the most recent performance review, within 5 working days of receipt Approaching Target – 90% successful response rate to SOW issued up to the date of the most recent performance review, within 5 working days of receipt Requires Improvement – 85-90% successful response rate to SOW issued up to the date of the most recent performance review, within 5 working days of receipt Inadequate – <85% successful response rate to SOW issued up to the date of the most recent performance review, within 5 working days of receipt	The service level measure is **'Good'** across a 3-month period.	Rectification Plan Process pursuant to Clause 31 is followed.
Successful delivery of Deliverables in accordance with their corresponding Acceptance Criteria against the specified	The supplier delivers the outcomes agreed in each work package in line with the acceptance criteria and milestone dates	**Good** –up to the most recent performance review, 90-100% of Statements of Work have been signed off as been delivered in accordance with their corresponding Deliverables and Acceptance Criteria against the specified Milestone Dates. Where SoW have not been fulfilled by the specified milestone date for circumstances reasonably determined to be within the	The service level measure is **'Good'** across a 3-month period.	Rectification Plan Process pursuant to Clause 31 is followed.

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
Milestone Dates.		Supplier's control, they are remedied within a time period agreed with the Authority. **Approaching Target** – up to the most recent performance review, 80-90% of Statements of Work have been signed off as been delivered in accordance with their corresponding Deliverables and Acceptance Criteria against the specified Milestone Dates. Where SoW have not been fulfilled by the specified milestone date for circumstances reasonably determined to be within the Supplier's control, they are remedied within a time period agreed with the Authority. **Requires Improvement** – up to the most recent performance review, 70-80% of Statements of Work have been signed off as been delivered in accordance with their corresponding Deliverables and Acceptance Criteria against the specified Milestone Dates. Where SoW have not been fulfilled by the specified milestone date for circumstances reasonably determined to be within the Supplier's control, they are remedied		

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
		within a time period agreed with the Authority. **Inadequate** – up to the most recent performance review, 0-70% of Statements of Work have been signed off as been delivered in accordance with their corresponding Deliverables and Acceptance Criteria against the specified Milestone Dates. Where SoWs have not been fulfilled by the specified milestone date for circumstances reasonably determined to be within the Supplier's control, they are remedied within a time period agreed with the Authority. Or: Where SoWs have not been fulfilled by the specified milestone date for circumstances reasonably determined to be within the Supplier's control, they are not remedied by the time period agreed with the Authority.		
Quality of individuals provided to deliver outcomes agreed	The resource provided as part of the Supplier's response to a Statement of Work are of sufficient	Good – 0 personnel swap-outs across the SOW period due to the resource not meeting the Key Indicator descriptions. No training or intervention required from the Authority staff for activities, technologies or practices etc that		Rectification Plan Process pursuant to Clause 31 is followed.

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
	quality, experience and expertise. They require no training for activities, technologies or practices etc that they are reasonably expected to be proficient in.	they are reasonably expected to be proficient in. Approaching Target – 1 personnel swap-outs across the SOW period due to the resource not meeting the Key Indicator descriptions. No training or intervention required from the Authority staff for activities, technologies or practices etc that they are reasonably expected to be proficient in. Requires Improvement – 2- 3 personnel swap-outs across the SOW period due to the resource not meeting the Key Indicator descriptions. No training or intervention required from the Authority staff for activities, technologies or practices etc that they are reasonably expected to be proficient in. Inadequate – 3 or more swap-outs across the SOW period due to the resource not meeting the Key Indicator descriptions. Or Training or intervention required from the Authority staff for activities, technologies or practices etc that		

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
		they are reasonably expected to be proficient in. Subject to all active SOW's over a monthly period.		
Social Value KPI – Tackling Workforce Inequality	Identify and tackle inequality in employment, skills and pay in the contract workforce and Supplier's own organisation	**Good:** Method Statement as detailed in Supplier's response to the Social Value Question at ITT stage is kept to. The supplier can demonstrate that, in line with timelines specified in the Method Statement, that "action is agreed upon. The action could come in the form of a positive action scheme, a pay review, the identification of training, or a change in policy. The director who conducted the audit is responsible for the actions. All the directors then have a chance to feedback on the process and methods." The supplier demonstrates, on a quarterly basis, that the Method Statement is being acted upon. By each performance review, the supplier provides a further report on the "Related Practices and Activities" that have transpired since contract start which demonstrate measures are being taken to meet the Tackling Workforce Inequality Key Indicator. Reporting relating to the metrics defined above are delayed by no more than 5 working days**.**	The service level measure is **'Good'** across a 3-month period.	Rectification Plan Process pursuant to Clause 31 is followed.

Service Levels				Rectification Measures
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
		Approaching Target: Activities and reporting relating to the metrics defined in “good” are delayed by 6-10 working days. **Requires Improvement:** Activities and reporting relating to the metrics defined in “good” are delayed by 11-20 working days. **Inadequate:** Activities and reporting relating to the metrics defined in “good” are delayed by more than 20 working days.		

Crown Commercial Service

Critical Service Level Failure

Critical Service Level Failure shall include a significant impact to Departmental operations for services that are dependent upon the successful delivery of Statements of Work completed via this contract, during the overall time period of any individual related work package.

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

.1.5 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
Not Applicable		

Part B – Key Sub-Contractors

[Guidance Note: *Insert details of Key Sub-Contractors and any additional information required in the below table or delete the table in its entirety and insert Not Applicable if there are no Key Sub-Contractors. This table should be based on the Key Sub-Contractors set out in Schedule 7 of the Framework*]

Key Sub-contractor name and address (if not the same as the registered office)	Registered office and company number	Related product/Service description	Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period	Key role in delivery of the Services
Magia CX UK Limited*	08557311	Oracle Consultancy Service Provider	90% of the total projected Charges over the Contract Period	100% of the service provision

*For the avoidance of doubt, the Subprocessor for this Call-Off is Magia CX UK Limited

Crown Commercial Service

Attachment 6 – Software

.1.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

.1.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software

The Supplier Software includes the following items:

Software	Supplier (if an Affiliate of the Supplier)	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry

Part B – Third Party Software

Crown Commercial Service

The Third Party Software shall include the following items:

Third Party Software	Supplier	Purpose	Number of Licences	Restrictions	Number of Copies	Type (COTS or Non-COTS)	Term/ Expiry

Attachment 7 – Financial Distress [NOT APPLICABLE]

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Operational Board	
Buyer Members for the Operational Board	To be confirmed
Supplier Members for the Operational Board	To be confirmed
Frequency of the Operational Board	To be confirmed
Location of the Operational Board	To be confirmed

PART B – LONG FORM GOVERNANCE [NOT APPLICABLE]

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 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 Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: Emma Wharram

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

Deputy Director - Departmental Data Protection Officer

Email: dataprotection.office@education.gov.uk

Address: Department for Education (B2.28), 7 & 8 Wellington Place, Wellington Street, Leeds, LS1 4AW

1.1.1.2 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.3 Any such further instructions shall be incorporated into this Attachment 9.

c	Details
Identity of Controller for each Category of Personal Data	**The Authority is Controller, and the Supplier is Processor** The Parties acknowledge that in accordance with Clause 34.2 to 34.15 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: Personal Data such as provider names, email addresses, telephone numbers, addresses or any other such data that is processed as detailed in each Statement of Work for the purposes of fulfilling contract delivery. **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, • Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under this Contract. *e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer*

Duration of the processing	12/12/2022 – 11/12/2022 (with possible extension for 1 year)
Nature and purposes of the processing	Details of the nature and purposes of personal data processing will be set out in the individual Statements of Works. Processing may include but is not limited to the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and/or erasure or destruction of data (whether or not by automated means). The precise nature and purpose of the processing will be defined in the individual Statements of Work. Personal data processing will include: • That which is processed through the platforms utilised for contract delivery. • That which is processed in the delivery of services as set out at Attachment 1 – Services Specification. • That which is processed in accordance with the individual Statement of Works
Type of Personal Data	As defined in each Statement of Work: May include but not be limited to: Names, Addresses, Email Addresses, Telephone Numbers
Categories of Data Subject	Staff, Providers, Provider 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	It is not expected that the Data Processor will retain any personal data processed through the platforms utilised in the delivery of this contract. If this is required, it will be clearly set out in the individual Statement of Work. Any data retained must be in accordance with DfE's agreed retention policies. The data security clauses within the contract must be adhered to for all data handling, deletion and destruction.

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
[Performance]			
[Charges]			
[Key Sub-Contractors]			
[Technical]			
[Performance management]			

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

A: Ethical Walls Agreement

DEPARTMENT FOR EDUCATION

and

BRAMBLE HUB LTD

ETHICAL WALLS AGREEMENT

This Agreement is dated 12th December 2022

Between

(1) **Department for Education** (the **"Authority"**) acting on behalf of the Crown of 20 Great Smith St, London SW1P 3BT; and

(2) **Bramble Hub Limited** a company registered in England and Wales under registered number 04136381whose registered office is at 9e Albert Embankment, London, SE1 7SP (the **"Counterparty"**).

together the "**Parties**" and each a "**Party**".

BACKGROUND

A. The Authority is obliged to ensure transparency, fairness, non-discrimination and equal treatment in relation to its procurement process pursuant to the Public Contracts Regulations 2015 (as amended) (the **PCR)**. The purpose of this document ("Agreement") is to define the protocols to be followed to prevent, identify and remedy any conflict of interest (whether actual, potential or perceived) in the context of the Procurement.

B. The Authority is conducting a procurement exercise for the supply of Data Science Services – Oracle Intelligent Advisor (the **"Purpose"**).

C. The Authority has an obligation to deal with conflicts of interest as set out in Regulation 24 (1) of the PCR. The concept of conflict of interest is wide. In the PCR it is described as covering at least *"any situation where relevant staff members have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure"* (Regulation 24(2)). *"Staff members"* refers to staff members of the Authority or of a procurement service provider acting on behalf of the Authority who are involved in the conduct of the procurement procedure or may influence the outcome of that procedure*. "Procurement service provider"* refers to a public or private body which offers ancillary purchasing activities on the market.

D. Pursuant to Regulation 41 of the PCR, the Authority is under an obligation to ensure that competition is not distorted by the participation of any bidder. Accordingly, the Authority has identified that a potential distortion of competition could arise as a consequence of a bidder wishing to submit a Tender for this procurement, where it has also performed services for the

Authority under existing contractual arrangements or as a subcontractor under those same arrangements.

E. The parties wish to enter into this Agreement to ensure that a set of management processes, barriers and disciplines are put in place to ensure that conflicts of interest do not arise, and that the Counterparty does not obtain an unfair competitive advantage over Other Bidders.

IT IS AGREED:

1 DEFINITIONS AND INTERPRETATION

1.1 The following words and expressions shall have the following meanings in this agreement and its recitals:

"**Affiliate**" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

"**Agreement**" means this ethical walls agreement duly executed by the Parties;

"**Bid Team**" means any Counterparty, Affiliate, connected to the preparation of an ITT Response;

"**Central Government Body**" means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:

a) Government Department;
b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);
c) Non-Ministerial Department; or
d) Executive Agency;

"**Conflicted Personnel**" means any Counterparty, Affiliate, staff or agents of the Counterparty or an Affiliate who, because of the Counterparty's relationship with the Authority under any Contract have or have had access to information which creates or may create a conflict of interest;

"**Contract**" means the contract for Data Science Services – Oracle Intelligent Advisor dated 12/12/2022 between the Authority and the Counterparty and/or an Affiliate;

"**Control**" means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and "**Controls**" and "**Controlled**" shall be interpreted accordingly;

"**Effective Date**" means the date of this Agreement as set out above;

"**Invitation to Tender**" or "**ITT**" means an invitation to submit tenders issued by the Authority as part of an ITT Process;

"**ITT Process"** means, with regard to the Purpose, the relevant procedure provided for in the PCR which the Authority has elected to use to select a contractor, together with all relevant information, correspondence and/or documents issued by the Authority as part of that procurement exercise, all information, correspondence and/or documents issued by the bidders in response together with any resulting contract;

"ITT Response" means the tender submitted or to be submitted by the Counterparty or an Affiliate [(or, where relevant, by an Other Bidder)] in response to an ITT;

"Other Affiliate" any person who is a subsidiary, subsidiary undertaking or holding company of any Other Bidder;

"Other Bidder" means any other bidder or potential bidder that is not the Counterparty or any Affiliate that has or is taking part in the ITT Process;

"Parties" means the Authority and the Counterparty;

"**Professional Advisor**" means a supplier, subcontractor, advisor or consultant engaged by the Counterparty under the auspices of compiling its ITT Response;

"**Purpose**" has the meaning given to it in recital B to this Agreement;

"**Representative"** refers to a person's officers, directors, employees, advisers and agents and, where the context admits, providers or potential providers of finance to the Counterparty or any Affiliate in connection with the ITT Process and the representatives of such providers or potential providers of finance; and

"**Third Party**" means any person who is not a Party and includes Other Affiliates and Other Bidders.

1.2 Reference to the disclosure of information includes any communication or making available information and includes both direct and indirect disclosure.

1.3 Reference to the disclosure of information, or provision of access, by or to the Authority or the Counterparty includes disclosure, or provision of access, by or to the representatives of the Authority or Representatives of the Counterparty (as the case may be).

1.4 Reference to persons includes legal and natural persons.

1.5 Reference to any enactment is to that enactment as amended, supplemented, re-enacted or replaced from time to time.

1.6 Reference to clauses and recitals is to clauses of and recitals to this Agreement.

1.7 Reference to any gender includes any other.

1.8 Reference to writing includes email.

1.9 The terms “associate”, “holding company”, “subsidiary”, “subsidiary undertaking” and “wholly owned subsidiary” have the meanings attributed to them in the Companies Act 2006, except that for the purposes of section 1159(1)(a) of that Act, the words ‘holds a majority of the voting rights’ shall be changed to ‘holds 30% or more of the voting rights’, and other expressions shall be construed accordingly.

1.10 The words “include” and “including” are to be construed without limitation.

1.11 The singular includes the plural and vice versa.

1.12 The headings contained in this Agreement shall not affect its construction or interpretation.

2 ETHICAL WALLS

2.1 In consideration of the sum of £1 payable by the Authority to the Counterparty, receipt of which is hereby acknowledged, the Counterparty:

2.1.1 shall take all appropriate steps to ensure that neither the Counterparty nor its Affiliates and/or Representatives are in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Counterparty or its Affiliates or Representatives and the duties owed to the Authority under the Contract or pursuant to an open and transparent ITT Process;

2.1.2 acknowledges and agrees that a conflict of interest may arise in situations where the Counterparty or an Affiliate intends to take part in the ITT Process and, because of the Counterparty’s relationship with the Authority under any Contract, the Counterparty, its Affiliates and/or Representatives have or have had access to information

which could provide the Counterparty and/or its Affiliates with an advantage and render unfair an otherwise genuine and open competitive ITT Process; and

2.1.3 where there is or is likely to be a conflict of interest or the perception of a conflict of interest of any kind in relation to the ITT Process, shall comply with Clause 2.2.

2.2 The Counterparty shall:

2.2.1 Not assign any of the Conflicted Personnel to the Bid Team at any time;

2.2.2 Provide to the Authority a complete and up to date list of the Conflicted Personnel and the Bid Team and reissue such list upon any change to it;

2.2.3 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates results in information of any kind or in any format and however so stored:

(a) about the Contract, its performance, operation and all matters connected or ancillary to it becoming available to the Bid Team; and/or

(b) which would or could in the opinion of the Authority confer an unfair advantage on the Counterparty in relation to its participation in the ITT Process becoming available to the Bid Team;

2.2.4 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates and in particular the Bid Team results in information of any kind or in any format and however so stored about the ITT Process, its operation and all matters connected or ancillary to it becoming available to the Conflicted Personnel;

2.2.5 Ensure that confidentiality agreements which flow down the Counterparty's obligations in this Agreement are entered into as necessary between the Authority and the Counterparty, its Affiliates, its staff, agents, any Conflicted Personnel, and between any other parties necessary in a form to be prescribed by the Authority;

2.2.6 physically separate the Conflicted Personnel and the Bid Team, either in separate buildings or in areas with restricted access;

2.2.7 provide regular training to its staff, agents and its Affiliates to ensure it is complying with this Agreement;

2.2.8 monitor Conflicted Personnel movements within restricted areas (both physical and electronic online areas) to ensure it is complying with this Agreement ensure adherence to the ethical wall arrangements;

2.2.9 ensure that the Conflicted Personnel and the Bid Team are line managed and report independently of each other; and

2.2.10 comply with any other action as the Authority, acting reasonably, may direct.

2.3 In addition to the obligations set out in Clause 2.1.1 and 2.1.3, the Counterparty shall:

2.3.1 notify the Authority immediately of all perceived, potential and/or actual conflicts of interest that arise;

2.3.2 submit in writing to the Authority full details of the nature of the conflict including (without limitation) full details of the risk assessments undertaken, the impact or potential impact of the conflict, the measures and arrangements that have been established and/or are due to be established to eliminate the conflict and the Counterparty's plans to prevent future conflicts of interests from arising; and

2.3.3 seek the Authority's approval thereto,

which the Authority shall have the right to grant, grant conditionally or deny (if the Authority denies its approval the Counterparty shall repeat the process set out in clause 2.3 until such time as the Authority grants approval or the Counterparty withdraws from the ITT Process).

2.4 Any breach of Clause 2.1, Clause 2.2 or Clause 2.3 shall entitle the Authority to exclude the Counterparty or any Affiliate or Representative from the ITT Process, and the Authority may, in addition to the right to exclude, take such other steps as it deems necessary where, in the reasonable opinion of the Authority there has been a breach of Clause 2.1, Clause 2.2 or Clause 2.3.

2.5 The Counterparty will provide, on demand, any and all information in relation to its adherence with its obligations set out under Clauses 2.1 and 2.2 as reasonably requested by the Authority.

2.6 The Authority reserves the right to require the Counterparty to demonstrate the measures put in place by the Counterparty under Clauses 2.1.3 and 2.2.

2.7 The Counterparty acknowledges that any provision of information or demonstration of measures, in accordance with Clauses 2.5 and 2.6, does not constitute acceptance by the Authority of the adequacy of such measures and does not discharge the Counterparty of its obligations or liability under this Agreement.

2.8 The actions of the Authority pursuant to Clause 2.4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

2.9 In no event shall the Authority be liable for any bid costs incurred by:

2.9.1 the Counterparty or any Affiliate or Representative; or

2.9.2 any Other Bidder, Other Affiliate or Other Representative,

as a result of any breach by the Counterparty, Affiliate or Representative of this Agreement, including, without limitation, where the Counterparty or any Affiliate or Representative, or any Other Bidder, Other Affiliate or Other Representative are excluded from the ITT Process.

2.10 The Counterparty acknowledges and agrees that:

2.10.1 neither damages nor specific performance are adequate remedies in the event of its breach of the obligations in Clause 2; and

2.10.2 in the event of such breach by the Counterparty of any of its obligations in Clause 2 which cannot be effectively remedied the Authority shall have the right to terminate this Agreement and the Counterparty's participation in the ITT Process.

3 SOLE RESPONSIBILITY

3.1 It is the sole responsibility of the Counterparty to comply with the terms of this Agreement. No approval by the Authority of any procedures, agreements or arrangements provided by the Counterparty or any Affiliate or Representative to the Authority shall discharge the Counterparty's obligations.

4 WAIVER AND INVALIDITY

4.1 No failure or delay by any Party in exercising any right, power or privilege under this Agreement or by law shall constitute a waiver of that or any other right, power or privilege, nor shall it restrict the further exercise of that or any other right, power or privilege. No single or partial exercise of such right, power or privilege shall prevent or restrict the further exercise of that or any other right, power or privilege.

4.2 If any provision of this Agreement is prohibited or unenforceable in any jurisdiction in relation to any Party, such prohibition or unenforceability will not invalidate the remaining provisions of this Agreement or affect the validity or enforceability of the provisions of this Agreement in relation to any other Party or any other jurisdiction.

5 ASSIGNMENT AND NOVATION

5.1 Subject to Clause 5.2 the Parties shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Authority.

5.2 The Authority may assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:

5.2.1 any Central Government Body; or

5.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority; and

5.2.3 the Counterparty shall, at the Authority's request, enter into a novation agreement in such form as the Authority may reasonably specify in order to enable the Authority to exercise its rights pursuant to this Clause 5.

5.3 A change in the legal status of the Authority such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Authority.

6 CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

6.1 A person who is not a Party to this Agreement has no right under the Contract (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any term of this Agreement but this does not affect any right remedy of any person which exists or is available otherwise than pursuant to that Act.

7 TRANSPARENCY

7.1 The parties acknowledge and agree that the Authority is under a legal duty pursuant to the PCR to run transparent and fair procurement processes. Accordingly, the Authority may disclose the contents of this Agreement to potential bidders in the ITT Process, for the purposes of transparency and in order to evidence that a fair procurement process has been followed.

8 NOTICES

8.1 Any notices sent under this Agreement must be in writing.

8.2 The following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

Manner of Delivery	Deemed time of service	Proof of service
Email	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message.
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt.
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next working day service providing proof of delivery.	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

.2

8.3 Notices shall be sent to the addresses set out below or at such other address as the relevant party may give notice to the other party for the purpose of service of notices under this Agreement:

	Counterparty	Authority
Contact		
Address		
Email		

.3

8.4 This Clause 8 does not apply to the service of any proceedings or other documents in any legal action or other method of dispute resolution.

9 WAIVER AND CUMULATIVE REMEDIES

9.1 The rights and remedies under this Agreement may be waived only by notice and in a manner that expressly states that a waiver is intended. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

9.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

10 TERM

10.1 Each party's obligations under this Agreement shall continue in full force and effect for period of 3 years from the Effective Date.

11 GOVERNING LAW AND JURISDICTION

11.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.

11.2 The Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

Signed by the Authority	Name: Signature: Position in Authority:
Signed by the Counterparty	Name: Neil Simpson Signature: Position in Counterparty:Director

B: Commercial Policy Guidance – Supplier Expenses: Travel and Subsistence

The Model Services Contract Schedules clearly states that "reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Authority's expenses policy current from time to time." Therefore, it is understood that the authority's expenses policy applies for the supplier.
Reimbursement does not include:

- expenses incurred as a result of Supplier Personnel travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Authority otherwise agrees in advance in writing
- subsistence expenses incurred by Supplier Personnel whilst performing the Services at their usual place of work

Supporting documentation

To claim for a reimbursement supporting document such as a receipt is needed to be made payable. Sufficient information is required to enable the Authority reasonably to assess whether the Charges, Reimbursable Expenses, and other sums due from the Authority detailed in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts.

- Supplier should keep record of the expenses incurred and a record of relevant records with each invoice.
- If the Authority requests copies of such records, the Supplier shall make them available to the Authority within 10 Working Days of the Authority's request.

Please see the Model Services Agreement Combined - Schedule 15 for further guidance.

Department for Education expenses policy for DfE contractor use

- Keep all receipts for any items you intend to claim; scan, photograph or otherwise digitally record them as soon as possible, to ensure you have an electronic copy. Without receipts, your claim can be refused.

Rail travel: Train journeys must be made by the cheapest available route and should be booked in advance where possible to secure the cheapest rates.

You can only buy a first-class train ticket if it is:

- recommended for you in accordance with workplace reasonable adjustments (to be agreed with DfE Contract Manager)
- the cheapest for the journey (screenshot proof must be provided)

Hotel rates: London max £135, outside London max £75. Approval is needed if room is above rate.

Subsistence:

Period of absence from permanent place of work	Receipted actuals up to a limit of
Over 5 hours and there is no food provided: 1 meal.	£4.50
Over 10 hours and there is no food provided: 2 meals.	£9.30

Over 12 hours and there is no food provided: 3 meals.	£13.80
Over 24 hours and breakfast is included in the hotel rate.	£21.25
If breakfast is NOT included in hotel rate, then you have the maximum cost of another meal added to the 24-hour allowance above.	£4.50
You have an allowance for breakfast on day 1 - if your official journey starts before 6.00am and is part of an overnight stay.	£4.50
If you are away more than 24 hours and staying with friends or family, you can claim receipted actuals for lunch and an evening meal	£21.25

Vehicle mileage rates:

Car

Up to 10,000 miles per year: 45p

Over 10,000 miles per year: 25p

Motorcycles

Up to 10,000 miles per year: 24p

Over 10,000 miles per year: 24p

Bicycles

Up to 10,000 miles per year: 20p

Over 10,000 miles per year: 20p

Taxis

You can take a taxi only if no other suitable method of transport is available.

Further Reading

Other guidance for reference includes Travel and Expenses Policy and

Claim expenses.

Part C –

(Buyer Specific Security Requirements)

1. Definitions

1.1. In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

"BPSS" "Baseline Personnel Security Standard"	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
"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 Legislation

"Buyer's Data" "Buyer's Information"	is any data or information owned or retained to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Buyer; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Buyer is the Data Controller;
"Departmental Security Requirements"	the Buyer's security policy or any standards, procedures, process or specification for security that the Supplier is required to deliver.
"Digital Marketplace / G-Cloud"	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
"End User Devices"	the personal computer or consumer devices that store or process information.
"Good Industry Standard" "Industry Good Standard"	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"	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"	Her Majesty's Government
"ICT"	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"	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 ICT system.
"Need-to-Know"	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"	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"	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"	the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction-0

"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	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"	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"	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
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under the Contract.

Operative Provisions

1.1. The Supplier shall be aware of and comply with the relevant HMG security policy framework, NCSC guidelines and where applicable these Departmental Security Requirements which include but are not constrained to the following paragraphs.

1.2. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 dated 25 May 2016, or any subsequent updated document, are mandated, 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 Buyer.

1.3. Where paragraph 1.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the Services supplied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

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

1.5. Buyer's Data being handled while providing an ICT solution or service must be separated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required in line with paragraph 1.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

1.6. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the products or Services, and that store or process Buyer's Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

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

1.8. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to:

1.8.1. physical security controls;

1.8.2. good industry standard policies and processes;

1.8.3. malware protection;

1.8.4. boundary access controls including firewalls, application gateways, etc;

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

1.8.6. use of secure device configuration and builds;

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

1.8.8. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;

1.8.9. any services provided to the Buyer must capture audit logs for security events in an electronic format at the application, service and system level to meet the Buyer's logging and auditing requirements, plus logs shall be:

1.8.9.1. retained and protected from tampering for a minimum period of six months;

1.8.9.2. made available to the Buyer on request.

1.9. The Supplier shall ensure that any Buyer's Data (including email) transmitted over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.

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

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

1.12. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer's 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 Buyer's 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 paragraph 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, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier’s assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier’s organisation in line with paragraph 1.15.

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

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-contractor protects) the Buyer’s Information and Buyer’s Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

1.16. Access by Supplier Staff to Buyer’s 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 Buyer. All Supplier Staff must complete this process before access to Buyer’s Data is permitted. [Any Supplier 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].

1.17. All Supplier Staff who handle Buyer’s Data shall have annual awareness training in protecting information.

1.18. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the Services delivered. If an 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 must include evidence that the Supplier has tested or exercised these plans within

the last 12 months and produced a written report of the outcome, including required actions.

1.19. Any suspected or actual breach of the confidentiality, integrity or availability of Buyer's Data, including user credentials, used or handled while providing the Services shall be recorded as a Security Incident. This includes any non-compliance with the Departmental Security Requirements and these provisions, or other security standards pertaining to the solution.

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

Security Incidents shall be reported through the Buyer's nominated system or service owner.

Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

1.20. The Supplier shall ensure that any Supplier ICT systems and hosting environments that are used to handle, store or process Buyer's Data, including Supplier ICT connected to Supplier ICT systems used to handle, store or process Buyer's 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 Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required, to be determined by the Buyer upon review of the ITHC findings.

1.21. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process or store Buyer's Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.

1.22. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services 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 Services being supplied and the Supplier's, and any sub-contractors', compliance with the paragraphs contained in this Schedule.

1.23. The Supplier 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 Buyer. This will include obtaining any necessary professional security resources required to support the Supplier'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.

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

1.24.1. compliance with HMG Minimum Cyber Security Standard.

1.24.2. any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification (e.g. United Kingdom Accreditation Service).

1.24.3. any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

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

Additional information and evidence to that listed above may be required to ensure compliance with DfE security requirements as part of the DfE security assurance process. Where a request for evidence or information is made by the Buyer, the Supplier will acknowledge the request within 5 working days and either provide the information within that timeframe, or, if that is not possible, provide a date when the information will be provided to the Buyer. In any case, the Supplier must respond to information requests from the Buyer needed to support the security assurance process promptly and without undue delay.

1.25. The Supplier shall contractually enforce all these Departmental Security Requirements onto any third-party suppliers, sub-contractors or partners who could potentially access Buyer's Data in the course of providing the Services.

1.26. The Supplier shall comply with the NCSC's social media guidance: how to use social media safely for any web and social media-based communications. In addition, any Communications Plan deliverable must include a risk assessment relating to the use of web and social media channels for the programme, including controls and mitigations to be applied and how the NCSC social media guidance will be complied with. The Supplier shall implement the necessary controls and mitigations within the plan and regularly review and update the risk assessment throughout the contract period. The Buyer shall have the right to review the risks within the plan and approve the controls and mitigations to be implemented, including requiring the Supplier to implement any additional reasonable controls to ensure risks are managed within the Buyer's risk appetite.

1.27. Any Supplier ICT system used to handle, store or process the Buyer's Data, including any Supplier ICT systems connected to systems that handle, store or process the Buyer's Data, must have in place protective monitoring at a level that is commensurate with the security risks posed to those systems and the data held. The Supplier shall provide evidence to the Buyer upon request of the protective monitoring arrangements in place needed to assess compliance with this requirement.