www.cqc.org.uk

Contract for the Provision of Enterprise Service Bus Application Support and Development Services

April 2018

FORM OF CONTRACT

PARTIES:

(1) THE CARE QUALITY COMMISSION of 3rd Floor, 151 Buckingham Palace Road, London, SW1W 9SZ (the "**Authority**");

AND

(2) Open Answers Ltd, a company registered in England under company number 02865597 and whose registered office is at 1-3 Tyburn Lane, Harrow, Middlesex, HA1 3AG (the "**Supplier**")

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

WHEREAS

A. This Contract is issued by the Authority in accordance with the VEAT Notice Reference 2018/S 054-120142 dated 17/03/2018.

B. The Contractor is knowledgeable and skilful in the field of ESB Services and an experienced contractor to the Authority

C. This Contract is for the provision of ESB Application Support and Development by the Contractor to the Authority and such other services as the Parties may from time to time agree under a Statement of Work.

NOW IT IS HEREBY AGREED as follows:

1. TERMS OF CONTRACT

1.1 The "**Contract**" comprises the following:

Part A - Contract Data

Part B - The Schedules
- Schedule 1 - Specification
- Schedule 2 – Service Levels
- Schedule 3 - Statement of Work (SOW), including pricing arrangements
- Schedule 4 - Contract Change Notice (CCN)
- Schedule 5 – Supplier's Code of Conduct
- Schedule 6 - Security Requirements, Policy and Plan
- Schedule 7 – Authority's Business Disaster Recovery Plan
- Schedule 8 – Processing, Personal Data and Data Subjects
- Schedule 9 – Supplier and Third Party Software
- Schedule 10 – Exit Plan
- Schedule 11- Key Performance Indicators (KPIs)

PART C – TERMS AND CONDITIONS

The Contract Data (Part A), the Schedules (Part B) and the Terms and Conditions (Part C) will become the binding Contract. The Contract Data may include:

1.2 The Contract starts on 01/04/2018 (the "**Commencement Date**") and ends on 31/03/2019 (the "**End Date**") the "Initial Period" unless it is terminated early or extended in accordance with the Contract.

1.3 The Authority may extend the term of the Contract until 31/03/2020 ("**Extension**"). The Authority may, by giving written notice to the Supplier not less than the three (3) Months prior to the last day of the Initial Contract Period, extend the Contract for further periods of up to a further 12 Months. Any such period shall not exceed a maximum extension of 12 Months. The terms of the Contract will apply throughout the period of any Extension.

Part A - Contract Data

Authority	Care Quality Commission
Supplier	Open Answers Limited
Contract/Project Ref.	ICTC CQC 769
Contract title	Enterprise Service Bus Application Support and Development
Contract description	ESB Application Support and Development
Contract period	12 Months
Start date	01/04/2018
End date	31/03/2019
Contract extension option	12 Months
Contract value	£210,000
Charging method	

Capped time and materials (CTM)	X
Price per story	
Time and materials (T&M)	
Fixed price	
Other pricing method or a combination of pricing methods agreed by the parties	

Notice period for termination for convenience	90 Days
Purchase order No.	
Initial SOW package	

Principle contact details

For the Authority:	Name:	[redacted]
	Title:	
	Email:	
For the Supplier	Name:	
	Title:	
	Email:	
	Phone:	

Contract term

Commencement date:	01/04/2018 and is valid for 12 months.

Authority contractual requirements

Warranty period	As stated in part C, Terms and Conditions
Location:	The Services will not primarily be performed on CQC premises but must be undertaken at Suppliers chosen location
Staff vetting procedures:	
Standards:	Both the Authority and the Contractor are committed to adhere to IT standards recognised as IT industry best practices and will continue to adapt to the changing IT industry standards, where appropriate and mutually agreed
Limit on Supplier's liability:	As set out in Clause 33.3 in Part C Terms and Conditions
Insurance:	As set out in Clause10 in Part C Terms and Conditions

Supplier's information

Commercially sensitive information:	All pricing information is commercially sensitive
Sub-contractors / Partners:	

Contract Charges and payment

The method of payment for the Contract Charges	BACS

Invoice details

Who and where to send invoices to:	Care Quality Commission T70 Payables F175 Phoenix House Topcliffe Lane Wakefield West Yorkshire WF3 1WE
Invoice information required	Purchase Order
Invoice frequency	Monthly
Contract value:	Minimum £210,000

Contract Charges:

The Contract Charges for Support will be billed monthly in arrears.

The Contract Charges for Development services shall be calculated monthly on a time and materials basis calculated using the rate card within Part B Schedule 1 Specification.

Formation of Contract

1.1 By signing and returning this Contract Data (Part A), the Supplier agrees to enter into a Contract with the Authority.

1.2 The parties agree that they have read the Contract Data (Part A) and the Contract terms and by signing below agree to be bound by this Contract.

1.3 The Contract outlines the Deliverables of the agreement. The Contract Data outlines any amendment within the terms and conditions of the Contract and will supersede the standard terms and conditions in the event of a conflict.

2. Background to the agreement

(A) The Supplier is a provider of ICT support and development services and undertook to provide such Services under the terms set out in this Contract.

(B) The Authority enters into this Contract with the Supplier in accordance with the VEAT Notice Reference 2018/S 054-120142 dated 17/03/2018 .

(C) The parties intend that this Contract will not itself oblige the Authority to buy or the Supplier to supply the Services. Specific instructions and requirements will have contractual effect on the execution of an SOW.

SIGNED:

	Supplier:	**Authority:**
Name:	Open Answers Ltd	Care Quality Commission
Title:	[redacted]	
Signature:		
Date:		

services to live operation. It includes the patching of those components as required to maintain support and to ensure reliable and secure operation of the platform.

Development is defined as software break/fix and software development services for enhancements and change requests.

The Authority will provide: specifications of requirements, acceptance criteria, wire frames, test data and other supporting material as may be necessary to provide a clear explanation of the requirements. The supplier will support CQC in doing this.

The Authority will perform System testing, User Acceptance testing, Regression testing, Load/performance testing, and Security testing as appropriate to meet the quality criteria for the overall deliverable. The Authority shall be deemed to have accepted the software when it commences live running of the whole or any part of the software (excluding the acceptance tests).

Version and components

The Integration Platform at CQC comprises the following components:

Platform Component	Versions	Function
Mule ESB EE (now known as Anypoint Platform)	3.8 LTS (PP) 3.8 LTS (OLS) 3.8 LTS (NRP/ADR/CCT)	Enterprise service bus (ESB) and integration platform
Apache ActiveMQ	5.10.0 (PP) 5.13.2 (OLS/NRP)	Messaging provider (reliable message queues)
Apache HTTP Server	2.2.15	HTTP server and reverse proxy
PostgreSQL	9.3.5	Relational database management system. Persistent storage for data (OLS and NRP) and messages queues
Neo4J CE	2.1.1	Graph database management system. Persistent storage for PP and Syndications API data, including ratings.
Mule Management Console (MMC)	3.6.0	Real-time monitoring, Flow Analyser, Debugging
Hawtio	1.4.62	Enhanced ActiveMQ Management Console
Apache Tomcat	6.0.35 (MMC) 7.0.67 (Hawtio)	Container for Mule Management Console (MMC)
389 Directory Server	1.2.11.15	LDAP server
Java Runtime Environment	1.8	Runtime environment for all Java Server based components, e.g. Mule, Tomcat, Neo4J

Location

Hosted by Atos at their Experian data centre.

Component Lifecycle Status

The Integration Platform and the capabilities it provides are a core part of CQC's information systems strategy and key to the effective integration of new products and services.

Business processes supported

CQC require support and development (as required) to ensure the following business processes run effectively:

- The transfer of data to Drupal to facilitate the publication of data in provider profiles.
- The Open Data initiative which provides an 'API' interface for any IT system with access to the Internet to consume CQC's publically available data.
- The Adult Social Care inspection publication process that provides the report data to Drupal as a series of XML files transported using SFTP and managing the web service request for a pdf report from Drupal to CRM.
- Provide the mechanism to transfer ratings information from the Secure Digital Publisher to OBIEE.
- The orchestration of information to support the Cygnum SaaS implementation.

Existing interfaces

Currently interfaces include:

- Drupal (CQC website) in order to send inspection report data and the pdf to Drupal using REST web services.
- Syndications Partners to provide facilities to retrieve Organisations data and ratings
- OBIEE in order to receive Provider Profile and inspections data using Informatica ETL processes and SFTP.
- Siebel CRM, using SOAP web services, to provide Adult Social Care inspection pdf reports to Drupal
- Siebel CRM, using SOAP web services, to integrate Organisations, Contacts and Enquiries data between CRM, the Provider Portal and SOAD Portal.
- MHAC-database, using SOAP web services, to integrate Enquiries data with the Provider Portal and SOAD Portal.
- The OLS database and LDAP in order to provide online digital identity facilities for users of the Provider Portal.

- Siebel CRM, using the MuleSoft Siebel Connector, to integrate Organisations, Contacts and Inspections data with Cygnum.
- Siebel CRM, using the MuleSoft Siebel Connector, to integrate Contacts, Enquiries and Attachments with the Contact Centre Telephony system (Storm).
- Provider Information Collection (PIC), to provide Contact search and Locations data synchronisation facilities, using data retrieved from OBIEE.
- Electronic Staff Records (ESR), to integrate Persons data with Cygnum.
- Secure Digital Publisher (SDP), through the consumption of an SDP XHTML file, translation to conform to an XML Schema and to OBIEE via SFTP
- Endeca, providing a facility for text information to be extracted for analysis from inspection reports and CRM attachments.
- Ordnance Survey, in order to provide address lookup facilities to Provider Portal and CRM.

- New interfaces
- The development of new interfaces may be required as and when new digital systems are developed, these will be developed in line with Digital priorities.
- Current and projected capacity
- No changes to the compute and storage capacity of the Integration Platform are projected.
- Network impact
- Minimal network impact is anticipated as any SFTP interfaces will be single thread and low volume, usually out of core hours. All other interfaces are low volume transactions.
- Data and information architecture
- The data that the Integration Platform transports relates to several elements of the logical data model although it does not currently actively support the model as it does not change the structure of that data.
- Mobility
- The Integration Platform is an enabling piece of infrastructure rather than an end user tool, as such it has no direct impact on mobility or home workers.
- Security
- Data is transported by the Integration Platform between known points that are deemed secure enough to hold OFFICIAL SENSITIVE information. It is not an end user tool and the access controls within Informatica are considered adequate to protect this data as they are restricted to systems engineers and developers and subject to independent testing before entering live service.

Detailed activity and supported API list.

This section lists API endpoints that are currently actively monitored (polled regularly with a synthetic transaction) in order to measure service availability.

Provider Profile API – Providers:

- Monitoring via the IMS3 network infrastructure and load balancer
- Monitor queries every minute requesting details of a sample provider

Provider Profile – Locations

- Monitor queries every minute requesting details of a sample location
- Syndications API
- Monitor queries every ten minutes requesting lists of all providers and locations

Online services

- Mule Authentication – monitor the service every minute
- OLS Mule get attachment (api.cqc.org.uk) monitors service every minute

NRP

- CRM activities
- Performance queries
- ESR FTPS connectivity /Pending files check monitors that the ESR FTPS server is accessible by the ESB
- ESR inbound API availability check

Incident Management

- ITSM incidents, OLS JIRA tickets and other
- Helpdesk

Problem Management

- Software support

Change and Release Management

- Change requests – ESB, Cygnum, PP Apps for PIC, Syndications and PP Apps – NRP and PIC
- Cross dependent change requests with CRM & OBIEE
- Platform upgrades
- Discovery work, requirements, scope, design and estimation
- Development sprints – test and feature development
- Iterative releases co-ordinated with CQC test teams activity
- Production deployment
- Project management and governance
- Service and systems integration

Capacity Management

- CPU usage across the main OLS and ESB servers
- Operations readiness/support model, systems monitoring

3. Service Levels

Severity Level	Initial Support response	Target Resolution Time	Coverage
Severity Level 1	30 Minutes	4 Hours	24x7 where P1 incident commences within core hours
Severity Level 2	1 Hour	6 Hours	During core hours
Severity Level 3	2 Hours	1 Working day	During core hours
Severity Level 4	1 Working Day	2 Working days	During core hours

Core hours are defined as being between 08:00am and 18:30pm on working days. The application support severity levels are defined below:

Severity Level	Description
Severity Level 1	Entire application and/or interface unavailable to all users and/or severe disruption to customers business
Severity Level 2	Specific modules of application and/or interface unavailable to all users and/or major disruption to customers business
Severity Level 3	Severe functionality defect and/or minor disruption to customers business
Severity Level 4	Minor functionality defect and/or minor disruption to customers business

3.Changes to delivery – Digital Transformation Support

To support the realisation of CQC's ambitions as set out in the Shaping the Future Strategy of 2016, the Digital and Intelligence teams are putting in place plans which will deliver a step-change in capability to enable CQC to become a more intelligence-driven, efficient and effective regulator.

The Strategy requires CQC moving away from a Waterfall model to an Agile approach to delivery. It requires a shift from building monolithic, difficult to change systems & processes, to a set of services that adopt a micro services architecture

ensuring interoperability between systems and a test driven approach that assures and facilitates change at pace.

The supplier will need to display flexibility in their approach to support CQC through this change and have both the capacity and capability to work with CQC to deliver effectively through new ways of working.

The change to ways of working may involve a new approach to the following although at this stage there is no commitment or timeframe to deliver these:

Change & Release Management

- Change requests – ESB, Cygnum, PP Apps for PIC, Syndications and PP Apps – NRP and PIC
- Cross dependent change requests with CRM & OBIEE
- Platform upgrades
- Discovery work, requirements, scope, design and estimation
- Development sprints – test and feature development
- Iterative releases co-ordinated with CQC test teams activity
- Production deployment
- Project management and governance
- Service and systems integration

CQC has longer term ambitions to migrate ESB to cloud and to develop an in-house development environment that will support collaborative ways of working with our suppliers. In order for this to be established CQC recognise that a period of knowledge transfer would be required.

During this contract CQC may look to explore how this knowledge transfer could take place in order to increase internal knowledge and to potentially build internal development capacity that can support and facilitate the need to deliver at pace.

If required, CQC would anticipate the knowledge transfer to involve and enable the following:

- 2 x suitably trained and skilled members of CQC staff to become configurators building up to bespoke implementation and support for the core infrastructure components of the platform, Mule ESB, PostgreSQL, Neo4J, ActiveMQ, Linux, LDAP
- Create the ability to debug Java code and Mule flows and understand CQC's data models.

Through the use of common standards, practices and toolsets, integration projects can be delivered consistently and in parallel by a number of different development teams whilst still being supported by a single resolver group

Transfer of knowledge activities and scope may include:

- Face to face knowledge transfer sessions
- Structured training/presentation on tools, processes & best practice guidance
- Reference documentation & Guided by third party

- Short term co-location opportunity
- Monthly/bi/monthly integration peer group meetings with developers
- Shadowing of Open Answers developers
- System monitoring
- Support requirements and operational escalation contacts
- Produce release notes and other documentation templates (supplied by Supplier)
- Business rules and relationships

If required, the transfer of knowledge activities, along with any dependent infrastructure setup will be initiated by CQC following the Change Request process.

4. Cost Envelope

Support & Maintenance Development
Application Support

Charges for Application Support will be paid monthly in Arrears on receipt of an Approved Invoice.

Application Support	Annual Charge Exc VAT
01/04/2018 – 01/04/2019	£210,000

Development T&M Rate Card

Resource Title	Standard G Cloud Rate	700 days	800 days	1000 days	1200 days	1500 days
Technical Design Authority (SFIA 7)	[redacted]					
Senior Archtiect (SFIA 6)						
Archtiect (SFIA 5)						
Senior Developer (SFIA 5)						
Developer (SFIA 4)						
Network Administrator (SFIA 4)						
Database Administrator (SFIA 4)						

Senior Systems Engineer (SFIA 5)	[redacted]					

Schedule 3 - Statement of Work (SOW), including pricing arrangements and Key Staff

Sch3.1 SOW Details

Date of SOW:	*Please enter the first date (on site)*
SOW Reference:	
Authority:	*Authority Full Name*
Supplier:	*Supplier Full Name*
Release Type(s):	*Please enter here*
Phase(s) of Development:	*Choose an item*
Release Completion Date:	*Please enter the Release Completion Date*
Duration of SOW	*Please enter the number of days here*
Charging Method(s) for this Release:	*Choose an item*

3.1.1 The Parties will execute a SOW for each release. Note that any ad-hoc Service requirements are to be treated as individual Releases in their own right (in addition to the releases at the delivery stage); and the Parties should execute a separate SOW in respect of each.

3.1.2 The rights, obligations and details agreed by the Parties and set out in this SOW apply only in relation to the Services that are to be delivered under this SOW and will not apply to any other SOW's executed or to be executed under this Contract unless otherwise agreed by the Parties.

Sch 3.2 Key Staff

3.2.1 The Parties agree that the Key Staff in respect of this Project are detailed in the table below.

3.2.2 Table of Key Staff:

Name	Role	Details

Sch 3.3 Deliverables

3.3.1 To be added in agreement between the Authority and Supplier

Sch 3.4 Contract Charges

3.4.1. For each individual Statement of Work (SOW), the applicable Contract Charges (in accordance with the charging method in the Contract Data) will be calculated using all of the following:

- the agreed relevant rates for Supplier staff or facilities, which are inclusive of any applicable expenses and exclusive of VAT and which were submitted to the Authority during the Further Competition that resulted in the award of this Contract.
- the number of days, or pro rata for every part of a day, that Supplier staff or facilities will be actively providing the Services during the term of the SOW.
- a contingency margin of up to 20% applied to the sum calculated on the basis of the above two points, to accommodate any changes to the SOW Deliverables during the term of the SOW (not applicable to Lot 3). The Supplier must obtain prior written approval from the Authority before applying any contingency margin.

3.4.2 The Supplier will provide a detailed breakdown of rates based on time and materials Charges, inclusive of expenses and exclusive of VAT, with sufficient detail to enable the Authority to verify the accuracy of the time and material Contract Charges incurred.

The detailed breakdown for the provision of Services during the term of the SOW may include (but will not be limited to):

- a role description per Supplier Staff;
- a facilities description;
- the agreed relevant rate per day;
- any expenses charged per day, which are in line with the Authority's expenses policy (if applicable);
- the number of days, or pro rata for every part day, they will be actively providing the Services during the term of the SOW; and
- the total cost per role / facility

The Supplier will also provide a summary which is to include:

- Total value of this SOW
- Overall Contract Charge
- Remainder of value under overall Contract Charge

Where: Remainder of value under overall Contract Charge = overall Contract Charge – sum of total value of all SOWs invoiced

- Whether there is any risk of exceeding Overall Contract Charge (and thereby requiring a Contract Change Note (CCN) to continue delivery of Services)

3.4.3 If a capped or fixed price has been agreed for a SOW:

- The Supplier will continue at its own cost and expense to provide the Services even where the agreed price has been exceeded; and
- The Authority will have no obligation or liability to pay for the cost of any Services delivered relating to this order after the agreed price has been exceeded.

3.4.4 Risks or contingencies will be included in the Charges. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges

3.4.6 Multiple SOWs can operate concurrently.

3.4.7 The Supplier will keep accurate records of the time spent by the Supplier staff in providing the services and will provide records to the Authority for inspection on request (not applicable to Lot 3 Services)

Sch 3.5. Agreement of statement of works

BY SIGNING this SOW, the parties agree to be bound by the terms and conditions set out herein:

For and on behalf of the Supplier: .....

Name and title .....

Signature and date

X .....

.....

For and on behalf of the Authority: .....

Name and title .....

Signature and date

X .....

.....

Please note that this is the first SOW. If the value of the first SOW is lower than the overall Contract value, and subsequent SOW(s) are required to ensure the Services are delivered, they must be raised and signed by the Authority and the Supplier

If you exceed the overall Contract value and Supplier Staff are still required to deliver the services, then a contract change note (CCN) must be raised, explaining the reason(s) for the extension.

Schedule 4 - Contract Change Notice (CCN)

Contract Data reference for the Contract being varied:

BETWEEN:

Care Quality Commission ("the Authority")

and

Open Answers Ltd ("the Supplier")

The Contract is varied as follows and shall take effect on the date signed by both Parties:

Guidance Note: Insert full details of the change including:

Reason for the change;

Full Details of the proposed change;

Likely impact, if any, of the change on other aspects of the Contract;

Words and expressions in this Contract Change Notice shall have the meanings given to them in the Contract.

The Contract, including any previous changes shall remain effective and unaltered except as amended by this change.

Signed by an authorised signatory for and on behalf of the Authority

Signature: _____

Date: _____

Name: _____

Address: _____

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature:

X _____

Date: _____

Name: _____

Address: _____

Schedule 5 – Government Commercial Function's Supplier Code of Conduct

https://www.gov.uk/government/publications/supplier-code-of-conduct

SCHEDULE 6 - SECURITY REQUIREMENTS, POLICY AND PLAN

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 6, unless the context otherwise requires the following provisions shall have the meanings given to them below:

"Breach of Security" means the occurrence of unauthorised access to or use of the Premises, the Services, the Supplier System, or any ICT or data (including Authority Data) used by the Authority or the Supplier in connection with the Contract.

"Supplier Equipment" means the hardware, computer and telecoms devices and equipment supplied by the Supplier or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

"Supplier Software" means software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services and which is specified as such in Schedule 9.

"ICT" means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

"Protectively Marked" shall have the meaning as set out in the Security Policy Framework.

"Security Plan" means the Supplier's security plan prepared pursuant to paragraph 3 an outline of which is set out in an Appendix to this Schedule 6.

"Software" means Specially Written Software, Supplier Software and Third Party Software.

"Specially Written Software" means any software created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Contract.

"Third Party Software" means software which is proprietary to any third party which is or will be used by the Supplier for the purposes of providing the Services including the software and which is specified as such in Schedule 9.

1. *INTRODUCTION*

This Schedule 6 covers:

1.1 principles of security, derived from the Security Policy Framework, including without limitation principles of physical and information security;

1.2 wider aspects of security relating to the Services;

1.5 breaches of security.

2 *PRINCIPLES OF SECURITY*

The CQC ESB is an Authority System that the Supplier provides software development services for and supports on its behalf.

In addition to the software components that Open Answers manages, the security of the Authority System is dependent on factors outside of Open Answers control including (but not limited to) :-

1. The network, server and storage infrastructure that the ESB is hosted on.
2. The security controls and security monitoring implemented within the infrastructure and networks.
3. The data that other Authority systems send to the ESB.
4. The authentication and authorisation controls for APIs that the Authority requires for each use case.
5. The ability to restrict external connections to the ESB from trusted network locations.
6. Ensuring that Authority staff and partners do not share access credentials for secure APIs.
7. Ensuring that the Authority implements effective starters and leavers processes for named accounts used for API access that are created by its staff and partners.
8. Ensuring that the Authority System and its components are appropriately tested by CQC – to include end-to-end system testing and security testing.

2.1 The Supplier acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Authority System. The Supplier also acknowledges the confidentiality of Authority Data.

2.2 The Supplier shall at all times, where possible, provide a level of security which:

2.2.1 is in accordance with Good Industry Practice and Law;

2.2.2 complies with Security Policy Framework; and

2.2.3 meets any specific security threats to the Authority System.

2.3 Without limiting paragraph 2.2, the Supplier shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):

2.3.1 loss of integrity of Authority Data;

2.3.2 loss of confidentiality of Authority Data;

2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;

2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Supplier in the provision of the Services;

2.3.5 use of the Authority System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.

2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

The Supplier will support the Authority in creating and executing its security plan.

4. NOT USED

5. NOT USED

6. BREACH OF SECURITY

6.1 Either Party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, authority data or services.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Supplier shall immediately take all reasonable steps necessary to:

6.2.1 remedy such breach or protect the Authority System against any such potential or attempted breach or threat; and

6.2.2 prevent an equivalent breach in the future;

6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;

6.2.4 investigate the incident and produce a detailed report for the Authority within 5 working days of the discovery of the incident.

6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Supplier under the Contract, then the Supplier shall be entitled to refer the matter to the CCN procedure set out in Schedule 4.

6.4 The Supplier shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

7. CONTRACT EXIT – SECURITY REQUIREMENTS

7.1 In accordance with clause 27 of the Contract, on termination of the Contract, either via early termination or completion of the Contract then the Supplier will either return all data to the Authority or provide a certificate of secure destruction using an industry and Authority approved method. Destruction or return of the data will be specified by the Authority at the time of termination of the Contract.

ANNEX 1: BASELINE SECURITY REQUIREMENTS

1. HIGHER CLASSIFICATIONS

1.1 The Supplier shall not handle Authority Data and information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Authority.

2. END USER DEVICES

2.1 When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.2 With the exception of Internet exposed APIs, devices used to access or manage Authority Data and services must be under the management authority of the Authority or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Supplier devices are expected to meet the set f security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--).

2.3 Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

3.1 The Supplier and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. Such approval shall not be unreasonably withheld or delayed unless specified otherwise in this Agreement and provided that storage, processing and management of any Authority Data are only carried out offshore within:

3.2.1 the European Economic Area (EEA);

3.2.2 in the US if the Supplier and or any relevant Sub-Contractor have signed up to the US-EU Privacy Shield Register; or

3.2.3 in another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the EU Commission.

3.3 The Supplier shall:

3.3.1 provide the Authority with all Authority Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Supplier authored assets in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 Securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority.

4. NETWORKING

4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

4.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY ARCHITECTURES

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Authority Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification(http://www.cesg.gov.uk/awarenesstraining/IA certification/Pages/index.aspx) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. PERSONNEL SECURITY

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work. The Supplier will not be liable for the costs of these checks but will be responsible for informing the Authority as when these checks need undertaking.

6.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Authority Data.

6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

6.4 All Supplier Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

6.5 Where the Supplier or Sub-contractors grants increased ICT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

ANNEX 2: SECURITY POLICY

[INSERT CQC SECURITY POLICY HERE]

ANNEX 3 – SECURITY MANAGEMENT PLAN

Schedule 7 - Authority's Business Disaster Recovery Plan

Schedule 8 – Processing, Personal Data and Data Subjects

For purposes of this Schedule, Contractor shall have the same meaning as Supplier and the Authority shall have the same meaning as the Client or Customer as defined in the Agreement.

1. The Contractor shall comply with any further written instructions with respect to processing by the Authority.

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	The ESB processes data relating to all of the subject matters across CQC's operating model and also of data relating mental health act responsibilities.
Duration of the processing	There is a persisted data store in the ESB for data transmitted to the public website. This is refreshed daily.
Nature and purposes of the processing	The ESB resides at the core of CQC's application architecture and brokers the messaging between all other processing applications. It also exposes CQC's data for external consumption and sharing via APIs. It therefore handles CQC's data for the purposes of the services it interacts with. The functionality of ESB has been specified by CQC and built into the system by Open Answers.
Type of personal data	This information relates to staff information as well as service user and provider data. This includes confidential personal information within some or all of these categories.
Categories of Data Subject	• CQC staff • Provider Staff and temporary workers • Suppliers • Service Users Citizens

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	The data handled by the ESB is stored and processed within the CQC environment (Atos Servers) and will therefore remain available at end points of origin or destination.

Schedule 9 – Supplier and Third Party Software

SUPPLIER AND THIRD PARTY SOFTWARE

SUPPLIER SOFTWARE

For the purposes of this Schedule 9, "**Supplier Software**" means software which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services. The Supplier Software comprises the following items:

Software	Supplier (if Affiliate of the Supplier)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
OAMon Event Relay		**System Monitoring**					**No**

THIRD PARTY SOFTWARE

For the purposes of this Schedule 9, "**Third Party Software**" means software which is proprietary to any third party which is or will be used by the Supplier for the purposes of providing the Services including the software specified in this Schedule 9. The Third Party Software shall consist of the following items:

Third Party Software	Supplier	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

Schedule 10 – Exit Plan

The supplier will maintain an up to date exit management plan and will share with the Authority when requested.

Schedule 11- Key Performance Indicators (KPIs)

Part C – Terms and conditions

1. CONTRACT START DATE, LENGTH AND METHODOLOGY

1.1 The Supplier will start providing the Services in accordance with the dates specified in any Statement of Work (SOW).

1.2 Completion dates for Deliverables will be set out in any SOW.

1.3 The term of this Contract will end on the Contract period end date listed in the Contract Data, or the latest completion date for a Deliverable specified in the final SOW (unless terminated earlier), whichever is the soonest.

1.4 Projects may need a combination of both waterfall and agile methods, playing to their respective strengths.

2. SUPPLIER STAFF

2.1 The Supplier Staff will:

(i) fulfil all reasonable requests of the Authority;

(ii) apply all due skill, care and diligence to the provisions of the Services;

(iii) be appropriately experienced, qualified and trained to supply the Services;

(iv) respond to any enquiries about the Services as soon as reasonably possible; and

(v) complete any necessary vetting procedures specified by the Authority.

2.2 The Supplier will ensure that Key Staff are assigned to provide the Services for their Working Days (agreed between Supplier and Authority) and are not removed from the Services during the dates specified in the relevant SOW.

2.3 The Supplier will promptly replace any Key Staff that the Authority reasonably considers unsatisfactory at no extra charge. The Supplier will promptly replace anyone who resigns with someone who is acceptable to the Authority. If the Supplier cannot provide an acceptable replacement, the Authority may terminate this Contract subject to clause 23.

2.4 Supplier Staff will comply with Authority requirements for the conduct of staff when on Authority's premises.

2.5 Where applicable, the Supplier will comply with the Authority's staff vetting procedures for all or part of the Supplier Staff.

2.6 Not Used

2.7 The Supplier must adhere to the Government Commercial Function - Supplier Code of Conduct appended hereto in Schedule 5.

2.8 This code exists to help Suppliers understand the standards

3. SWAP-OUT

3.1 Not Used

4. STAFF VETTING PROCEDURES

4.1 Where applicable, all Supplier Staff will need to be cleared to the level determined by the Authority prior to the commencement of work.

4.2 The Authority may stipulate differing clearance levels for different roles during this Contract period.

4.3 The Supplier will ensure where possible that it complies with any additional staff vetting procedures as requested by the Authority at no cost to the Supplier

5. DUE DILIGENCE

5.1 Both parties acknowledge that information will be needed to provide the Services throughout the term of this Contract and any periods of extension. Both parties agree to share such information freely.

5.2 Further to 5.1, both Parties agree that when entering into a Contract, they:

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

5.2.2 are confident that they can fulfil their obligations according to the terms of the Contract;

5.2.3 have raised all due diligence questions before the Contract; and

5.2.4 have entered into the Contract relying on its own due diligence.

6. WARRANTIES, REPRESENTATIONS AND ACCEPTANCE CRITERIA

6.1 The Supplier will use the best applicable and available techniques and standards and will perform this Contract with all reasonable care, skill and diligence, and according to Good Industry Practice, subject to any relevant constraints placed on it by the Authority.

6.2 The Supplier warrants that all Supplier Staff assigned to the performance of the Services will have the necessary qualifications, skills and experience for the proper performance of the Services.

6.3 The Supplier represents and undertakes to the Authority that each Deliverable will meet the Authority's acceptance criteria, where defined in the requirements, Contract Data or any applicable SOW.

6.4 The Supplier undertakes to maintain any interface (within its control) and interoperability between third-party software or Services and software or Services

developed by the Supplier, in accordance with any agreed specifications and Change Requests issued by the Authority.

6.5 The Supplier warrants that it has full capacity and authority and all necessary authorisations, consents, licences and permissions to perform this Contract.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY

7.1 If required by the Authority, the Supplier will ensure a disaster recovery approach is captured in a clear disaster recovery plan. All Supplier Staff must also adhere to the Authority's business continuity and disaster recovery procedure as required in the delivery of the Services for this project.

8. PAYMENT TERMS AND VAT

8.1 The Authority will pay the Supplier within 30 days of receipt of a valid invoice submitted in accordance with this Contract.

8.2 The Supplier will ensure that each invoice contains the information specified by the Authority in the Contract Data.

8.3 The Contract Charges are deemed to include all Charges for payment processing.

8.4 All payments under this Contract are inclusive of VAT.

9. RECOVERY OF SUMS DUE AND RIGHT OF SET-OFF

9.1 If a Supplier owes money to the Authority or any Crown body, the Authority may deduct that sum from the total due.

10. INSURANCE

The Supplier will maintain the insurances required by the Authority including those set out in this clause.

10.1 Sub-contractors

10.1.1 The Supplier will ensure that, during this Contract, Sub-contractors hold third-party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £5,000,000.

10.2 Agents and professional consultants

10.2.1 The Supplier will also ensure that all agents and professional consultants involved in the supply of Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Contract, and for 6 years after the termination or expiry date to this Contract to which the insurance relates.

10.3 Additional or extended insurance

10.3.1 If requested by the Authority, the Supplier will obtain additional insurance policies, or extend existing insurance policies procured under the Contract.

10.3.2 The Supplier will provide the Authority, the following evidence that they have complied with clause 10.3.1 above:

(i) a broker's verification of insurance; or
(ii) receipts in respect of the insurance premium; or
(iii) other evidence of payment of the latest premiums due.

10.4 Supplier liabilities

10.4.1 Insurance will not relieve the Supplier of any liabilities under the Contract.

10.4.2 Without limiting the other provisions of the Contract, the Supplier will:

(i) take all risk control measures relating to the Services as it would be reasonable to expect of a Supplier acting in accordance with Good Industry Practice, including the investigation and reports of claims to insurers;
(ii) promptly notify the insurers in writing of any relevant material fact under any insurances of which the Supplier is, or becomes, aware; and
(iii) hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of placing cover representing any of the insurance to which it is a Party.

10.4.3 The Supplier will not do or omit to do anything, which would entitle any insurer to refuse to pay any claim under any of the insurances.

10.5 Indemnity to principals

10.5.1 Where specifically outlined in this Contract, the Supplier will ensure that the third-party public and products liability policy will contain an 'indemnity to principals' clause under which the Authority will be compensated for both of the following claims against the Authority:

(i) death or bodily injury; and
(ii) third-party Property damage arising from connection with the Services and for which the Supplier is legally liable.

10.6 Cancelled, suspended, terminated or un-renewed policies

10.6.1 The Supplier will notify the Authority as soon as possible if the Supplier becomes aware that any of the insurance policies have been, or are due to be, cancelled, suspended, terminated or not renewed.

10.7 Premium, excess and deductible payments

10.7.1 Where any insurance requires payment of a premium, the Supplier will:

(i) be liable for the premium; and
(ii) pay such premium promptly.

10.7.2 Where any insurance is subject to an excess or deductible below the Supplier will be liable for it. The Supplier will not be entitled to recover any sum paid for insurance excess or any deductible from the Authority.

11. CONFIDENTIALITY

11.1 Except where disclosure is clearly permitted by this Contract, neither Party will disclose the other Party's Confidential Information without the relevant Party's prior written consent.

11.2 Disclosure of Confidential Information is permitted where information:

(a) must be disclosed to comply with legal obligations placed on the Party making the disclosure;
(b) belongs to the Party making the disclosure (who is not under any obligation of confidentiality) before its disclosure by the information owner;
(c) was obtained from a third party who is not under any obligation of confidentiality, before receiving it from the disclosing Party;
(d) is, or becomes, public knowledge, other than by breach of this clause or Contract;
(e) is independently developed without access to the other Party's Confidential Information; or
(f) is disclosed to obtain confidential legal professional advice.

11.3 The Authority may disclose the Supplier's Confidential Information:

(a) to any central government body on the basis that the information may only be further disclosed to central government bodies;
(b) to the UK Parliament, Scottish Parliament or Welsh or Northern Ireland Assemblies, including their committees;
(c) if the Authority (acting reasonably) deems disclosure, on a confidential basis, necessary or appropriate while carrying out its public functions;
(d) on a confidential basis to exercise its rights or comply with its obligations under this Contract; or
(e) to a proposed transferee, assignee or novatee of, or successor in title to, the Authority.

11.4 References to disclosure on a confidential basis will mean disclosure subject to a confidentiality agreement or arrangement containing the same terms as those placed on the Authority under this clause.

11.5 The Supplier may only disclose the Authority's Confidential Information to Supplier Staff who are directly involved in the provision of the Services and who need to know the information to provide the Services. The Supplier will ensure that its Supplier Staff will comply with these obligations.

11.6 Either Party may use techniques, ideas or knowledge gained during this Contract unless the use of these things results in them disclosing the other Party's Confidential Information where such disclosure is not permitted by the Contract, or is an infringement of Intellectual Property Rights.

12. CONFLICT OF INTEREST

12.1 The Supplier shall take appropriate steps to ensure that neither the Supplier nor any Staff is placed 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 Supplier and the duties owed to the Authority under the provisions of the Contract. The Supplier will notify the Authority without delay giving full particulars of any such conflict of interest which may arise.

12.2 The Authority may terminate the Contract immediately by notice and/or take or require the Supplier to take such other steps it deems necessary if, in the Authority's reasonable opinion, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under the provisions of the Contract. The actions of the Authority pursuant to this clause 12 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

13. INTELLECTUAL PROPERTY RIGHTS

13.1 Unless otherwise specified in this Contract:

13.1.1 the Authority will not have any right to the Intellectual Property Rights (IPRs) of the Supplier or its licensors, including the Supplier Background IPRs and any IPRs in the Supplier Software;

13.1.2 the Authority may publish any Deliverable that is software as open source;

13.1.3 the Supplier will not, without prior written approval from the Authority, include any Supplier Background IPR or third party IPR in any Deliverable in such a way to prevent its publication;

(i) and failure to seek prior approval gives the Authority right and freedom to use all Deliverables;

13.1.4 the Supplier will not have any right to the Intellectual Property Rights of the Authority or its licensors, including:

(i) the Authority Background IPRs;

(ii) the Project-Specific IPRs; and
(iii) IPRs in the Authority Data.

13.2 Where either Party acquires, by operation of Law, right to IPRs that is inconsistent with the allocation of rights set out above, it will assign in writing such IPRs as it has acquired to the other Party on the request of the other Party (whenever the request is made).

13.3 Except where necessary for the performance of this Contract (and only where the Authority has given its prior approval), the Supplier will not use or disclose any of the Authority Background IPRs, Authority Data or the Project-Specific IPRs to or for the benefit of any third party.

13.4 The Supplier will not include any Supplier Background IPRs or third-party IPRs in any release or Deliverable that is to be assigned to the Authority under this Contract, without approval from the Authority.

13.5 The Supplier will grant the Authority a perpetual, transferable, sub-licensable, non-exclusive, royalty-free licence to copy, modify, disclose and use the Supplier Background IPRs for any purpose connected with the receipt of the Services that is additional to the rights granted to the Authority under this Contract and to enable the Authority:

13.5.1 to receive the Services;
13.5.2 to make use of the Services provided by the replacement Supplier; and
13.5.3 to use any Deliverables.

13.6 The Authority grants the Supplier a non-exclusive, non-assignable, royalty-free licence to use the Authority Background IPRs, the Authority Data and the Project-Specific IPRs during the term of this Contract for the sole purpose of enabling the Supplier to provide the Services.

13.7 The Authority gives no warranty as to the suitability of any IPRs licensed to the Supplier hereunder. Any such licence:

13.7.1 may include the right to grant sub-licences to Sub-contractors engaged in providing any of the Services (or part thereof) provided that any such Sub-contractor has entered into a confidentiality undertaking with the Supplier on the same terms as in clause 11 (Confidentiality) and that any such subcontracts will be non-transferable and personal to the relevant Sub-contractor; and

13.7.2 is granted solely to the extent necessary for the provision of the Services in accordance with this Contract. The Supplier will ensure that the Sub-contractors do not use the licensed materials for any other purpose.

13.8 At the end of the term of this Contract, the Authority grants to the Supplier a licence to use the Project-Specific IPRs (excluding any information which is the Authority's Confidential Information or which is subject to the Data Protection Act (DPA)) on the terms of the Open Government Licence v3.0.

13.9 Subject to the above paragraph, the Supplier will ensure that no unlicensed software or open source software (other than the open source software specified by the Authority) is interfaced with or embedded within any Authority Software or Deliverable.

13.10 Before using any third-party IPRs related to the supply of the Services, the Supplier will submit to the Authority for approval, all details of any third-party IPRs the Authority requests.

13.11 Where the Supplier is granted permission to use third-party IPRs in a request for approval, the Supplier will ensure that the owner of such third-party IPRs grants to the Authority a licence on the terms informed to the Authority in the request for approval.

13.12 If the third-party IPR is made available on terms equivalent to the Open Government Licence v3.0, the request for approval will be agreed and the Supplier will buy licences under these terms. If not, and the Authority rejects the Request for Approval, then this Contract will need to be varied in accordance with clause 29 'Changes to Services'.

13.13 The Supplier will, on written demand, fully indemnify the Authority losses which it may incur at any time as a result of any claim (whether actual alleged asserted and/or substantiated and including third party claims) that the rights granted to the Authority in accordance with this Contract or the performance by the Supplier of the provision of the Services or the possession or use by the Authority of the Services or Deliverables delivered by the Supplier, including the publication of any Deliverable that is software as open source, infringes or allegedly infringes a third party's Intellectual Property Rights (an 'IPR Claim').

13.14 Clause 13.13 will not apply if the IPR Claim arises from:

(i) designs supplied by the Authority;
(ii) the use of data supplied by the Authority which is not required to be verified by the Supplier under any provision of this Contract; or
(iii) other material provided by the Authority necessary for the provision of the Services.

13.15 The indemnity given in Clause 13.13 will be capped up to the value of the contract

13.16 The Authority will notify the Supplier in writing of the IPR Claim made against the Authority for the contracted software or service and the Authority will not make any admissions which may be prejudicial to the defence or settlement of the IPR Claim. The Supplier will at its own expense conduct all negotiations and any litigation arising in connection with the IPR Claim provided always that the Supplier:

13.16. 1 consults the Authority on all substantive issues which arise during the conduct of such litigation and negotiations;
13.16.2 takes due and proper account of the interests of the Authority;
13.16.3 considers and defends the IPR Claim diligently using competent counsel and in such a way as not to bring the reputation of the Authority into disrepute; and
13.16.4 does not settle or compromise the IPR Claim without the prior approval of the Authority (such decision not to be unreasonably withheld or delayed).

13.17 If an IPR Claim is made (or in the reasonable opinion of the Supplier is likely to be made) in connection with this Contract, the Supplier will, at the Supplier's own expense and subject to prompt approval of the Authority, use its best endeavours to:

(i) modify the relevant part of the Services or Deliverables without reducing their functionality or performance, or substitute Services or Deliverables of equivalent functionality or performance, to avoid the infringement or the alleged infringement, provided that there is no additional cost or burden to the Authority;
(ii) buy a licence to use and supply the Services or Deliverables, which are the subject of the alleged infringement, on terms which are acceptable to the Authority; and

(iii) promptly perform any responsibilities and obligations to do with this Contract.

13.18 If an IPR Claim is made (or in the reasonable opinion of the Supplier is likely to be made) against the Supplier, the Supplier will immediately notify the Authority in writing.

13.19 If the Supplier does not comply with provisions of this clause within 20 Working Days of receipt of notification by the Supplier from the Authority under clause 13.16 or receipt of the notification by the Authority from the Supplier under clause 13.18 (as appropriate), the Authority may terminate this Contract for Material Breach (Contract) and the Supplier will, on demand, refund the Authority with all monies paid for the Service or Deliverable that is subject to the IPR Claim

13.20 The Supplier will have no rights to use any of the Authority's names, logos or trademarks without the Authority's prior written approval.

13.21 Both parties will, as an enduring obligation throughout the term of this Contract where any software is used in the provision of the Services or information uploaded, interfaced or exchanged with the Authority systems, use software and the most up-to-date antivirus definitions from an industry-accepted antivirus software vendor. It will use the software to check for, contain the spread of, and minimise the impact of Malicious Software (or as otherwise agreed between the Authority and the Supplier).

13.22 If Malicious Software is found, the Supplier will co-operate with the Authority to reduce the effect of the Malicious Software. If Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, the Supplier will use all reasonable endeavours to help the Authority to mitigate any losses and restore the provision of the Services to the desired operating efficiency as soon as possible.

13.23 Any costs arising from the actions of the Authority or Supplier taken in compliance with the provisions of the above clause, will be dealt with by the Authority and the Supplier as follows:

(i) by the Supplier, where the Malicious Software originates from the Supplier Software or the Authority Data while the Authority Data was under the control of the Supplier, unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier;

(ii) by the Authority if the Malicious Software originates from the Authority Software or the Authority Data, while the Authority Data was under the control of the Authority. For the avoidance of doubt, all data that enters the ESB from third party systems shall be deemed to be under the control of the Authority.

13.24 All Deliverables that are software shall be created in a format, or able to be converted into a format, which is suitable for publication by the Authority as open source software, unless otherwise agreed by the Authority.

13.25 Where Deliverables that are software are written in a format that requires conversion before publication as open source software, the Supplier shall also

provide the converted format to the Authority unless the Authority agrees in advance in writing that the converted format is not required.

14. DATA PROTECTION AND PRIVACY

14.1 The Supplier shall (and shall procure that its entire Staff) comply with any notification requirements under Data Protection Legislation and both Parties will duly observe all their obligations under Data Protection Legislation which arise in connection with the Contract.

14.2 The Supplier will, in conjunction with the Authority, in its own right and in respect of the Services, shall ensure it will be compliant with the provisions of the GDPR and Data Protection Legislation.

14.3 The Supplier shall designate and will provide the Authority with the contact details of its data protection officer where this position is required by the Data Protection Legislation or other designated individual with responsibility for data protection and privacy to act as the point of contact for the purpose of observing its obligations in this Clause 14.

14.4 Notwithstanding the obligations in clause 14.1 if the Supplier is Processing Personal Data as a Data Processor for the Authority, the Supplier shall:

(a) Prior to the processing of any Personal Data under this Contract and where requested by the Authority provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment ("DPIA"). Such assistance may, at the discretion of the Authority include (but not be limited to):

i. A systematic description of the envisaged processing operations and the purpose of the processing;
ii. An assessment of the necessity and proportionality of the processing operations in relation to the Services;
iii. an assessment of the risks to the rights and freedoms of Data Subjects; and
iv. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

(b) implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected including the measures as are set out in Clause 15 (Authority Data) and Clause 20 (Security) and Schedule 6 (Security Requirements, Policy and Plan).

(c) Process the Personal Data only in accordance with Schedule 8 and/or written instructions from the Authority (which may be specific instructions or instructions of a general nature) as set out in the Contract or as otherwise

notified by the Authority unless the Supplier is required to do so otherwise by Law. If it is so required, the Supplier shall promptly notify the Authority before processing the Personal Data unless prohibited by Law;

(d) Process the Personal Data only to the extent and in such manner as is necessary for the provision of the Supplier's obligations under the Contract or as is required by Law or any Regulatory Body;

(e) Keep a record of all categories of processing activities carried out on behalf of the Authority, containing;

i) the categories of processing carried out on behalf of the Authority;

ii) where applicable, any transfers of Personal Data to Restricted Countries or an international organisation.

(f) Ensure that it has in place Protective Measures, which have been reviewed and approved by the Authority as appropriate to protect against a Data Loss Event having taken account of the:
(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

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

a. do not process Personal Data except in accordance with this Agreement (and in particular Schedule 8);

b. are aware of and comply with the Supplier's duties under this Clause 14 and Clauses 15 (Authority Data) and 11 (Confidentiality);

c. are subject to appropriate confidentiality undertakings with the Supplier or any relevant Sub-contractor;

d. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by this Contract; and

e. have undergone adequate training in the use, care, protection and handling of personal data (as defined in the Data Protection Legislation);

(h) not disclose or transfer the Personal Data to, or allow the processing of Personal Data by any Sub-Contractor and/or Affiliates for the provision of the Services without Approval;

(i) not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

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

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

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

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

(j) at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination of the Agreement unless the Supplier is required by Law to retain the Personal Data;

(k) notify the Authority within 48 hours if it:

a. receives from a Data Subject (or third party on their behalf):
   i. a Data Subject Access Request (or purported Data Subject Access Request);
   ii. a request to rectify, block or erase any Personal Data; or
   iii. any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
b. considers that any of the Authority's instructions from the Authority infringe the Data Protection Legislation;
c. receives any Regulator Correspondence or any other communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract; or
d. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
e. is required by Law to commit an act or omission to that would, but for Clause 14.10, constitute a breach of this Clause 14;
f. becomes aware of a Data Loss Event;

(l) The Supplier's obligation to notify under Clause 14.4(k) shall include the provision of further information to the Authority in phases, as details become available.

14.4A Notwithstanding the provisions of clauses 14.1 and 14.4, where the Supplier is Processing Personal Data for the Authority, the parties acknowledge that the Authority is the Data Controller and the Supplier is the Data Processor. The Supplier shall set out the scope, nature and purpose of the Processing by the Supplier, the duration of the Processing and the types of Personal Data and the categories of Data Subject in the form appended hereto in Schedule 8– Processing, Personal Data and Data Subject.

14.5 Taking into account the nature of the processing, the Supplier shall provide the Authority with full co-operation and assistance (within the timescales reasonably required by the Authority) in relation to either Party's obligations under Data

Protection Legislation or any complaint, communication or request made as referred to in Clause 14.4(k), including by promptly providing:

a. the Authority with full details and copies of the complaint, communication or request;
b. where applicable, such assistance as is reasonably requested by the Authority to enable the Authority to comply with the Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation; and
c. the Authority, on its request, with any Personal Data it holds in relation to a Data Subject;
d. assistance as requested by the Authority following any Data Loss Event; and
e. assistance as requested by the Authority with respect to any request from the Information Commissioner's Office (ICO), or any consultation by the Authority with the ICO;

14.6 The Supplier shall, if requested by the Authority, provide a written description of the measures that it has taken and technical and organisational security measures in place, for the purpose of compliance with its obligations pursuant to this Clause 14 and provide to the Authority copies of all documentation relevant to such compliance including, processing records, procedures, guidance, training and manuals.

14.7 The Supplier shall allow the Authority (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit, in accordance with clause 50 (Audit), and paragraph 5 of Schedule 6 the Supplier's Data Processing activities (and/or those of Staff) and comply with all reasonable requests or directions by the Authority to enable the Authority to verify and/or procure that the Supplier is in full compliance with its obligations under the Contract;

14.8. The Supplier shall not Process or otherwise transfer any Personal Data in or to any Restricted Country without the Authority's prior written consent. If, after the Effective Date, the Supplier or any Sub-contractor wishes to Process and/or transfer any Personal Data in or to any Restricted Country, the Supplier shall, in seeking consent, submit such information as the Authority's shall require in order to enable it to consider the request and acknowledges that such consent may be given subject to conditions which will, if appropriate, be incorporated into this Contract at the Supplier's cost and expense using the Change Control Procedure.

14.9 The Supplier will notify the Authority immediately, and in any event no later than 12 hours, after becoming aware of a Data Loss Event, in particular the notification will be made regardless as to whether or not the Supplier has established any unauthorised access or other harm has actually arisen from the event. Notification must not be delayed for the purpose of establishing the effects of an identified Data Loss Event. In particular the Supplier will;

i) when notifying the Authority of a Data Loss Event will describe the nature of the event including the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

ii) Cooperate fully with any Authority investigation into the Data Loss Event including but not limited to the causes and effects (actual or potential);

iii) (If applicable), provide immediate access to the Supplier's premises and systems for the purposes of any Authority investigation under Clause 14.4 ii above;

iv) Take all necessary actions to remedy the causes or adverse effects of the Data Loss Event and to ensure the protection of Personal Data from any further loss. Where the Supplier reasonably considers that immediate action is required to ensure the protection of personal data, or to prevent or mitigate a serious risk of harm, damage or loss to data subjects arising from a Data Loss Event, they may take such action without requiring prior authorisation from the Authority circumstances where it is not reasonably possible to seek or obtain such authorisation in a timely manner;

v) Not make any public statement of any kind without the prior Approval of the Authority;

vi) Where appropriate, provide all assistance necessary to enable the Authority to fulfil its obligations to notify the Information Commissioner within 72 hours after becoming aware of the Data Loss Event; and

vii) notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

14.10 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this clause 14. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

(a) the Authority determines that the processing is not occasional;
(b) the Authority determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
(c) the Supplier determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

14.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Supplier must:
(a) notify the Authority in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Authority;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 14 such that they apply to the Sub-processor; and

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

14.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

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

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

14.15 At the end of the Term or earlier termination of this Contract, at the Authority's request, the Contractor shall delete or return all Personal Data to the Authority and delete any copies of such Personal Data except where required to retain any copies by Law.

14.16 The Supplier shall comply at all times with Data Protection Legislation and shall not perform its obligations under the Contract in such a way as to cause the Authority to breach any of its applicable obligations under the Data Protection Legislation.

14.17 The Supplier shall use its reasonable endeavours to assist the Authority to comply with any obligations under the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Authority to breach any of the Authority's obligations under the Data Protection Legislation to the extent the Supplier is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

14.18 Subject to clause 33.3 The Supplier shall indemnify the Authority on a continuing basis against any and all Losses incurred by the Authority arising from the Supplier's Default under this Clause 14 and/or any failure by the Contractor or any Sub-Contractor to comply with their respective obligations under Data Protection Legislation. The indemnity doesn't apply to the extent that the Supplier breach is due to an Authority instruction.

14.19 Nothing in this Clause 14 shall be construed as requiring the Supplier or any relevant Sub-contractor to be in breach of any Data Protection Legislation.

14.20 The provision of this clause 14 applies during the Contract Period and indefinitely after its expiry

15. AUTHORITY DATA

15.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

15.2 The Supplier shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

15.3 To the extent that Authority Data is held and/or Processed by the Supplier, the Supplier shall supply Authority Data to the Authority as requested by the Authority in the format specified in the SOW.

15.4 The Supplier shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data.

15.6 The Supplier shall ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework.

15.7 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:

(a) require the Supplier (at the Supplier's expense) to restore or procure the restoration of Authority Data and the Supplier shall do so promptly; and/or

(b) itself restore or procure the restoration of Authority Data, and shall be repaid by the Supplier any reasonable expenses incurred in doing so. The total aggregate liability cap shall apply.

15.8 If at any time the Supplier suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Supplier shall notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take.

16. DOCUMENT AND SOURCE CODE MANAGEMENT REPOSITORY

16.1 The Supplier will comply with any reasonable instructions given by the Authority as to where it will store documents and source code, both finished and in progress, during the term of this Contract.

16.2 The Supplier will ensure that all items that are uploaded to any repository contain sufficient detail, code annotations and instructions so that a third-party developer with the relevant technical abilities within the applicable role would be able to understand how the item was created and how it works together with the other items in the repository within a reasonable timeframe.

17. NOT USED

18. FREEDOM OF INFORMATION (FOI) REQUESTS

18.1 The Supplier acknowledges that the Authority is subject to the requirements of the Freedom of Information Act (FoIA) and the Environmental Information Regulation (EIR).

18.2 The Supplier will help and co-operate with the Authority to enable it to comply with their Information disclosure obligations regarding this Contract.

18.3 The Supplier will in no event respond directly to a Request for Information under the FoIA.

18.4 The Supplier will note that the Information disclosed in response to a FoIA or EIR request may include its response. This may include attachments, embedded documents, any score or details of the evaluation of a response. The Supplier will be consulted before disclosure.

18.5 If the Supplier considers any part of its response to be confidential or commercially sensitive, the Supplier will:

(i) identify this Information
(ii) explain the potential implications of its disclosure, specifically addressing the public interest test as in the Folia
(iii) estimate how long it believes such Information will remain confidential or commercially sensitive

18.6 The Authority will then consider whether or not to withhold such Information from publication. Even where Information is identified as confidential or commercially sensitive, the Authority may be required to disclose such Information in accordance with the Folia or the EIR.

18.7 The Authority must form an independent judgement of whether the Supplier's Information is exempt from disclosure under the Folia or the EIR and whether the public interest favours disclosure or not. Suppliers must refer any request for Information, including requests relating to the procurement, to the Authority.

19. STANDARDS AND QUALITY

19.1 The Supplier will comply with any standards in this Contract with Good Industry Practice and the following methodologies:

19.1.1 Not Used

19.1.2 Not Used

19.1.3 Projects may need the best of both waterfall and agile methods, playing to their respective strengths.

19.1.4 Guidance can be found at:

(i) the service design manual - https://www.gov.uk/service-manual/agile
(ii) the technology code of practice - https://www.gov.uk/service-manual/technology/code-of-practice.html#using-the-technology-code-

of-practice

19.2 The Supplier will seek to support the Authority to :

(i) provide Services through successful Service Standard assessments https://www.gov.uk/service-manual/digital-by-default

(ii) develop Services based on open standards and accessible data protocols, to ensure they are interoperable https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles.

(iii) comply with any standards that are compulsory in government - http://standards.data.gov.uk/challenges/adopted.

20. SECURITY

20.1 If requested to do so by the Authority, the Supplier will, within 5 Working Days of the date of this Contract, develop, obtain Authority's approval of, maintain and observe a Security Management Plan and an Information Security Management System (ISMS) which, after Authority approval, will apply during the term of this Contract. Both the ISMS and the Security Management Plan will comply with the security policy of the Authority contained in Schedule 6 and protect all aspects of the Services and all processes associated with the delivery of the Services that are within the Supplier's control.

20.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry accepted antivirus software vendor to minimise the impact of Malicious Software.

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

20.4 The Supplier will immediately notify the Authority of any breach of security in relation to the Authority's Confidential Information. The Supplier will recover such Authority Confidential Information however it may be recorded.

20.5 Any system development by the Supplier must also aim to comply, where determined by the Authority to be applicable, with the government's '10 Steps to Cyber Security' guidance, available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

20.6 The Authority will specify any security requirements for this project in the Contract Data.

20.7 If requested by the Authority, the Supplier must support according to:

20.7.1 the Baseline Personnel Security Standard (BPSS). Additional levels of security clearance may include:

a) Security Check (SC)

b) Developed Vetting (DV)

c) Counter-Terrorist Check (CTC)

20.7.2 the Supplier assurance framework for contracts at the 'Official' information security level - https://www.gov.uk/government/publications/government-Supplier-assurance-framework

20.7.3 any relevant security guidance - https://www.gov.uk/government/collections/government-security

20.7.4 the Cyber Essentials scheme - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview)

20.7.5 the Government Security Classification - https://www.gov.uk/government/publications/government-security-classifications

All of the above guidance may change occasionally.

20.8 The Supplier shall be liable for, and shall indemnify the Authority against all Losses suffered or incurred by the Authority and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of Security (to the extent that such Losses were not caused by any act or omission by the Authority).In relation to this clause the liability shall be capped up to the value of the contract.

21. INCORPORATION OF TERMS

21.1 Upon the execution of a Statement of Work (SOW), the terms and conditions agreed in the SOW will be incorporated into this Contract.

22. MANAGING DISPUTES

22.1 When either Party notifies the other of a dispute, both Parties will attempt in good faith to negotiate a settlement as soon as possible.

22.2 Nothing in this procedure will prevents a Party from seeking any interim order restraining the other Party from doing any act or compelling the other Party to do any act.

22.3 If the dispute cannot be resolved, either Party will be entitled to refer it to mediation in accordance with the procedures below, unless:

22.3.1 the Authority considers that the dispute is not suitable for resolution by mediation; and/or

22.3.2 the Supplier does not agree to mediation.

22.4 The procedure for mediation is as follows:

22.4.1 A neutral adviser or mediator will be chosen by agreement between the Parties. If the Parties cannot agree on a mediator within 10 Working Days after a request by one Party to the other, either Party will as soon as possible, apply to the mediation provider or to the Centre for Effective Dispute Resolution (CEDR) to appoint a mediator. This application to CEDR must take place within 12 Working Days from the date of the proposal to appoint a mediator, or within 3 Working Days of notice from the mediator to either Party that they are unable or unwilling to act.

22.4.2 The Parties will meet with the mediator within 10 Working Days of the mediator's appointment to agree a programme for the exchange of all relevant information and the structure for negotiations to be held. The Parties may at any stage seek help from the mediation provider specified in this clause to provide guidance on a suitable procedure.

22.4.3 Unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it will be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings.

22.4.5 If the Parties reach agreement on the resolution of the dispute, the agreement will be reduced to writing and will be binding on the Parties once it is signed by their duly authorised representatives.

22.4.6 Failing agreement, either Party may invite the mediator to provide a non-binding but informative opinion in writing. Such an opinion will be provided without prejudice and will not be used in evidence in any proceedings relating to this Contract without the prior written consent of both Parties.

22.4.7 If the Parties fail to reach agreement in the structured negotiations within 60 Working Days of the mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the courts.

22.5 Either Party may request by written notice that the dispute is referred to expert determination if the dispute relates to:

(i) any technical aspect of the delivery of the digital services;
(ii) the underlying technology; or
(iii) otherwise is of a financial or technical nature.

22.6 An expert will be appointed by written agreement between the Parties, but if there's a failure to agree within 10 Working Days, or if the person appointed is unable or unwilling to act, the expert will be appointed on the instructions of the President of

the British Computer Society (or any other association that has replaced the British Computer Society).

22.7 The expert will act on the following basis:

22.7.1 they will act as an expert and not as an arbitrator and will act fairly and impartially;

22.7.2 the expert's determination will (in the absence of a material failure to follow the agreed procedures) be final and binding on the Parties;

22.7.3 the expert will decide the procedure to be followed in the determination and will be requested to make their determination within 30 Working Days of their appointment or as soon as reasonably practicable and the Parties will help and provide the documentation that the expert needs for the determination;

22.7.4 any amount payable by one Party to another as a result of the expert's determination will be due and payable within 20 Working Days of the expert's determination being notified to the Parties;

22.7.5 the process will be conducted in private and will be confidential; and

22.7.6 the expert will determine how and by whom the costs of the determination, including their fees and expenses, are to be paid.

22.8 Without prejudice to any other rights of the Authority under this Contract, the obligations of the Parties under this Contract will not be suspended, ceased or delayed by the reference of a dispute submitted to mediation or expert determination and the Supplier and the Supplier Staff will comply fully with the requirements of this Contract at all times.

23. TERMINATION

23.1 The Authority will have the right to terminate this Contract at any time by giving the notice to the Supplier specified in Part A, the Contract Data. The Supplier's obligation to provide the Services will end on the date set out in the Authority's notice.

23.2 The minimum notice period (expressed in Working Days) to be given by the Authority to terminate under this clause is set out in Part A (90 Working Days).

23.3 Partial days will be discounted in the calculation and the duration of the SOW will be calculated in full Working Days.

23.4 The Parties acknowledge and agree that:

(I) the Authority's right to terminate under this clause is reasonable in view of the subject matter of this Contract and the nature of the Service being provided.

(ii) the Contract Charges paid during the notice period given by the Authority in accordance with this clause are a reasonable form of compensation and are deemed to fully cover any avoidable costs or losses incurred by the Supplier which may arise either directly or indirectly as a result of the Authority exercising the right to terminate under this clause without cause.

(iii) Subject to clause 33 (Liability), if the Authority terminates this Contract without cause, they will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate such Loss. If the Supplier holds insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of such Loss, with supporting evidence of unavoidable Losses incurred by the Supplier as a result of termination.

23.5 The Authority will have the right to terminate or suspend this Contract at any time with immediate effect by written notice to the Supplier if:

(i) the Supplier commits a Supplier Default and if the Supplier Default cannot, in the opinion of the Authority, be remedied;
(ii) the Supplier commits any fraud;
(iii) fails to meet any of the Key Performance Indicator Targets as specified in Schedule 11 on at least 3 occasions within a 12-month rolling period; or
(iv) the Supplier has scored a 'red' status on any one of the 4 KPI Targets listed on the balanced scorecard, on at least 2 occasions within the Contract duration, or within a period of 3 months (whichever is the soonest).

Any Key Performance Indicators (KPIs) must be proposed by the Authority and defined explicitly as such in an SOW. For the avoidance of doubt, any service that is monitored and measured by the Contractor as part of its Application Support services is not a KPI.

23.6 Either Party may terminate this Contract at any time with immediate effect by written notice to the other if:

(i) the other Party commits a Material Breach of any term of this Contract (other than failure to pay any disputed amounts due under this Contract) and, if such breach is remediable, fails to remedy that breach within a period of 15 Working Days of being notified in writing to do so;

(ii) an Insolvency Event of the other Party occurs, or the other Party ceases or threatens to cease to carry on the whole or any material part of its business; or

(iii) a Force Majeure Event occurs for a period of more than 15 consecutive calendar days.

23.7 If a Supplier Insolvency Event occurs, the Authority is entitled to suspend or terminate this Contract.

23.8 Termination on change of Control

23.8.1 The Authority may terminate this Contract by giving notice in writing to the Supplier with immediate effect within 1 month of either:

(i) being notified in writing that a change of Control (within the meaning of Section 450 of the Corporation Tax Act 2010) has occurred or is being contemplated; or

(ii) where no notification has been made, the date that Authority becomes aware that a change of Control has occurred or is contemplated.

23.9 If the Authority determines at its absolute and sole discretion that the change is prohibited under the Regulations or, where approval has not been granted before the change of Control, if Authority reasonably believes that such change is likely to have an adverse effect on the provision of the Services.

23.10 Termination, suspension or expiry of this Contract will be without prejudice to any accrued rights, remedies or obligations of either Party.

23.11 If the Supplier commits any fraud it will be a Material Breach, and:

(i) the Authority may terminate this Contract; and

(ii) the Authority may fully recover from the Supplier any Losses incurred as a consequence up to the value of the contract.

23.12 **Termination without cause by the Authority**

23.12.1 The Authority will have the right, without cause and without liability to suspend or terminate the Contract or any provisions of any part of this Contract by giving at least 90 days written notice to the Supplier.

24. CONSEQUENCES OF TERMINATION

24.1 If the Authority contracts with another Supplier, the Supplier will comply with clause 28.

24.2 The rights and obligations of the Parties in respect of this Contract (including any executed SOWs) will automatically terminate upon the expiry or termination of this Contract, except those rights and obligations set out in clause 24.6.

24.3 At the end of the Contract period (howsoever arising), the Supplier must

(i) immediately return to the Authority:

- all Authority Data including all copies of Authority Software and any other software licensed by the Authority to the Supplier under this Contract;

- any materials created by the Supplier under this Contract where the IPRs are owned by the Authority;

- any items that have been on-charged to the Authority, such as consumables; and all Equipment provided to the Supplier pursuant to clause 41. This Equipment must be handed back to the Authority in good working order (allowance will be made for reasonable wear and tear).

(ii) immediately upload any items that are or were due to be uploaded to the repository when this Contract was terminated (as specified in clause 27);

(iii) cease to use the Authority Data and, at the direction of the Authority, provide the Authority and the replacement Supplier with a complete and uncorrupted version of the Authority Data in electronic form in the formats and on media agreed with the Authority and the replacement Supplier;

(iv) destroy all copies of the Authority Data when they receive the Authority's written instructions to do so or 12 months after the date of expiry or termination, and provide written confirmation to the Authority that the data has been destroyed, except where the retention of Authority Data is required by Law;

(v) vacate the Authority premises;

(vi) work with the Authority on any work in progress and ensure an orderly transition of the Services to the replacement Supplier;

(vii) return any sums prepaid for Services which have not been delivered to the Authority by the date of expiry or termination;

(viii) provide all information requested by the Authority on the provision of the Services so that:

- the Authority is able to understand how the Services have been provided; and
- the Authority and the replacement Supplier can conduct due diligence.

24.4 Each Party will return all of the other Party's Confidential Information. Each Party will confirm that it does not retain the other Party's Confidential Information except where the information must be retained by the Party as a legal requirement or where this Contract states otherwise.

24.5 All licences, leases and authorisations granted by the Authority to the Supplier in relation to the Services will be terminated at the end of the Contract period (howsoever arising) without the need for the Authority to serve notice except where this Contract states otherwise.

24.6 Termination or expiry of this Contract will not affect:

(i) any rights, remedies or obligations accrued under this Contract prior to termination or expiration;

(ii) the right of either Party to recover any amount outstanding at the time of such termination or expiry;

(iii) the continuing rights, remedies or obligations of the Authority or the Supplier under clauses:

- 8 - Payment Terms and VAT

- 9 - Recovery of Sums Due and Right of Set-Off
- 11 - Confidentiality
- 12 - Conflict of Interest
- 13 - Intellectual Property Rights
- 14 – Data Protection and Privacy
- 20 - Security
- 24 - Consequences of Expiry or Termination
- 33 - Liability
- 34 - Waiver and cumulative remedies

(iv) any other provision of the Contract which expressly or by implication is to be performed or observed notwithstanding termination or expiry will survive the termination or expiry of this Contract.

25. SUPPLIER'S STATUS

25.1 The Supplier is an independent Supplier and no contract of employment or partnership is created between the Supplier and the Authority. Neither Party is authorised to act in the name of, or on behalf of, the other Party.

26. NOTICES

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

26.2 The following table sets out the method by which notices may be served under this Contract and the respective deemed time and proof of Service:

Delivery type	Deemed delivery time	Proof of Service
Email	9am on the first Working Day after sending	Dispatched in a pdf form to the correct email address without any error message

26.3 The address and email address of each Party will be the address and email address in the Contract Data.

27. EXIT PLAN

27.1 The Authority and the Supplier will agree an exit plan to be appended to this contract and transferred to the Authority ensuring that the Authority has all the code and documentation required to support and continuously develop the Service with Authority resource or any third party as the Authority requires. The Supplier will update this plan whenever there are material changes to the Services. A Statement of Work may be agreed between the Authority and the Supplier to specifically cover the exit plan.

28. HELP AT RETENDERING AND HANDOVER TO REPLACEMENT SUPPLIER

28.1 When requested, the Supplier will help the Authority to migrate the Services to a replacement Supplier in line with the exit plan (clause 27) to ensure continuity of the Services. Such help may include Supplier demonstrations of the existing code and development documents, software licences used and Authority approval documents. The

Supplier will also answer reasonable Service and development-related clarification questions.

28.2 Within 10 Working Days of a request by the Authority, the Supplier will provide any information needed by the Authority to prepare for any procurement exercise or to facilitate any potential replacement Supplier undertaking due diligence. The exception to this is where such information is deemed to be Commercially Sensitive Information, in which case the Supplier will provide the information in a redacted form.

29. CHANGES TO SERVICES

29.1 It is likely that there will be changes to the scope of the Services during the Contract period. Agile projects have a scope that will change over time. The detailed scope (e.g. as defined in user stories) can evolve and change during the Contract Period. These changes do not require formal contract changes but do require the Authority and Supplier to agree these changes.

29.2 Any changes to the high-level scope of the Services must be agreed between the Authority and Supplier. The Supplier will consider any request by the Authority to change the scope of the Services, and may agree to such request.

30. CONTRACT CHANGES

30.1 All changes to this Contract which cannot be accommodated informally as described in clause 29 will require a Contract Change Note.

30.2 Either Party may request a contract change by completing and sending a draft Contract Change Note in the form in Schedule 4 of Part B - The Schedules ('the **Contract Change Note**') to the other Party giving sufficient information to enable the other Party to assess the extent of the change and any additional cost that may be incurred. The Party requesting the contract change will bear the costs of preparation of the Contract Change Note. Neither Party will unreasonably withhold nor delay consent to the other Party's proposed changes to this Contract.

30.3 Due to the agile-based delivery methodology recommended by the Contract, it may not be possible to exactly define the consumption of Services over the duration of the Contract in a static Contract Data. The Supplier should state the initial value of all Services that are likely to be consumed under the Contract.

31. FORCE MAJEURE

31.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Contract to the extent that such delay or failure is a result of a Force Majeure event. Each Party will use all reasonable endeavours to continue to perform its obligations under this Contract for the length of a Force Majeure event. If a Force Majeure event prevents a Party from performing its obligations under this Contract for more than 15 consecutive calendar days, the other Party may terminate this Contract with immediate effect by notice in writing.

32. ENTIRE AGREEMENT

32.1 This Contract constitutes the entire agreement between the Parties relating to the matters dealt within it. It supersedes any previous agreement between the Parties relating to such matters.

32.2 Each Party agrees that in entering into this Contract it does not rely on, and will have no remedy relating to, any agreement or representation (whether negligently or innocently made) other than as expressly described in this Contract.

32.3 Nothing in this clause will exclude any liability for (or remedy relating to) fraudulent misrepresentation or fraud.

32.4 NOT USED

. 33. LIABILITY AND WARRANTY

33.1 Neither Party excludes or limits its liability for:

(i) death or personal injury;
(ii) bribery or fraud by it or its employees;
(iii) breach of any obligation as to title implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
(iv) any liability to the extent it cannot be excluded or limited by Law.

33.2 Not Used

33.3 Each Party's total aggregate liability relating to all Losses due to a Default in connection with this agreement:

- resulting in direct loss or damage to physical Property (including any technical infrastructure, assets or Equipment or IPR but excluding any loss or damage to the Authority Data or Authority's Personal Data of the other Party, will be limited to the annual contract value in each Contract year in which the Default occurs, unless otherwise stipulated by the Authority;

- subject to the first bullet point in this clause 33.3 which occur in the first 6 months, will be limited to the greater of the sum of £100,000 or a sum equal to 125% of the estimated Contract Charges for the first six months;

- subject to the first bullet point in this clause 33.3 which occur during the remainder of the Contract period, will be limited to the greater of the sum of £100,000 or an amount equal to 125% of the Contract Charges paid, due or which would have been payable under this Contract in the 6 months immediately preceding the event giving rise to the liability;

- Subject to the first bullet point, the annual aggregate liability for all Defaults resulting in direct loss, destruction, corruption degradation or damage to the Authority Data or Authority Personal Data or any copy of such

Authority Data, caused by the Supplier's Default under in connection with this Contract shall in no event exceed the value of the statutory regulatory fine.

- subject to the first bullet point in this clause 33.3 which occur after the end of the Contract period, will be limited to the greater of the sum of £500,000 or an amount equal to 125% of the Contract Charges paid, due or which would have been payable under this Contract in the 6 months immediately before the end of the Contract period.

33.4 Subject to clause 33.1, in no event will either Party be liable to the other for any:

(a) loss of profits;
(b) loss of business;
(c) loss of revenue;
(d) loss of or damage to goodwill;
(e) loss of savings (whether anticipated or otherwise); or
(f) any indirect, special or consequential loss or damage.

33.5 Subject to 33.3, the Supplier will be liable for the following types of loss which will be regarded as direct and will be recoverable by the Authority:

(a) the additional operational or administrative costs and expenses arising from any Material Breach; and/or

(b) any regulatory losses, fines, expenses or other losses arising from a breach by the Supplier of any Law.

33.6 No enquiry, inspection, approval, sanction, comment, consent, or decision at any time made or given by, or on behalf of, the Authority to any document or information provided by the Supplier in its provision of the Services, and no failure of the Authority to discern any defect in, or omission from, any such document or information will exclude or limit the obligation of the Supplier to carry out all the obligations of a professional Supplier employed in a client and Authority relationship.

33.7 Unless otherwise expressly provided, the obligations of the Authority under this Contract are obligations of the Authority in its capacity as a Contracting counterparty and nothing in this Contract will be an obligation on, or in any other way constrain the Authority in any other capacity, nor will the exercise by the Authority of its duties and powers in any other capacity lead to any liability under this Contract on the part of the Authority to the Supplier.

33.8 Any liabilities which are unlimited will not be taken into account for the purposes of establishing whether any limits relating to direct loss or damage to physical Property within this clause have been reached.

33.9 Nothing in this clause will exclude any liability for (or remedy relating to) fraud.

33.10 The Supplier warrants, represents and undertakes to the Authority all of the following:

(i) it has full capacity, authority and all necessary authorisations, consents,

licences, permissions, to enter into and perform its obligations under this Contract and each SOW.

(ii) the Supplier or an authorised representative will sign the Contract and each SOW;

(iii) in entering into the Contract it hasn't committed, or agreed to commit, a Prohibited Act before or after entering into the SOW;

(iv) the Contract shall be performed in compliance with all applicable UK Laws (as amended from time to time); and

(v) on the Commencement Date, all information, statements and representations contained in the Application for the Services are true, accurate and not misleading, save as may have been specifically disclosed in writing to the Authority prior to execution of the Contract, and the Supplier will advise the Authority of any fact, matter or circumstance of which it may become aware which would render any such information, statement or representation to be false or misleading; and all warranties, representations and undertakings contained in the Contract shall be deemed repeated in each SOW unless otherwise stated.

33.11 Any warranties in this Contract will not prevent any right of termination for its breach.

33.12 When entering into this Contract and each SOW, the Supplier confirms to the Authority that it has not committed any Fraud.

33.13 Nothing within this agreement relieves the Data Processor or Data Controller of their own direct responsibilities and liabilities under the GDPR. The parties accept that, in accordance with the GDPR, the ICO may administer an administrative fine against either the Data Controller or the Data Processor, depending on the circumstances and based on its determination of default, and the ICO does not permit fines which are imposed as a result of the Parties own direct default to be passed from the Controller to the Processor, or vice-versa."

34. WAIVER AND CUMULATIVE REMEDIES

34.1 The rights and remedies provided by this agreement may be waived only in writing by the Authority or the Supplier representatives in a way that expressly states that a waiver is intended, and such waiver will only be operative regarding the specific circumstances referred to.

34.2 Unless a right or remedy of the Authority is expressed to be exclusive, the exercise of it by the Authority is without prejudice to the Authority's other rights and remedies. Any failure to exercise, or any delay in exercising, a right or remedy by either Party will not constitute a waiver of that right or remedy, or of any other rights or remedies.

35. FRAUD

35.1 The Supplier will notify the Authority if it suspects that any fraud has occurred, or is likely to occur. The exception to this is if while complying with this, it would cause the Supplier or its employees to commit an offence.

35.2 If the Supplier commits any fraud relating to this Contract or any other contract with the government:

(a) the Authority may terminate the Contract; or

(b) the Authority may recover in full the contract value from the Supplier whether under Clause 35.3 below or by any other remedy available in law.

35.3 The Supplier will, on demand, compensate the Authority, in full, for any loss sustained by the Authority at any time (whether such loss is incurred before or after the making of a demand following the indemnity hereunder) in consequence of any breach of this clause.

36. PREVENTION OF BRIBERY AND CORRUPTION

36.1 The Supplier will not commit any Prohibited Act.

36.2 The Authority will be entitled to recover in full the contract value from the Supplier and the Supplier will, on demand, compensate (to the value of the contract) the Authority in full from and against:

(i) the amount of value of any such gift, consideration or commission.

37. LEGISLATIVE CHANGE

37.1 The Supplier will neither be relieved of its obligations under this Contract nor be entitled to increase the Contract prices as the result of a general change in Law or a Specific Change in Law without prior written approval from the Authority.

37.2 If a Specific Change in Law occurs during the term which has a material impact on the delivery of the Services or the Contract price range, the Supplier will notify Authority of the likely effects of that change. This will include whether any change is required to the Services, the Contract price range or this Contract.

38. PUBLICITY, BRANDING, MEDIA AND OFFICIAL ENQUIRIES

38.1 The Supplier will take all reasonable steps to not do anything which may damage the public reputation of the Authority. The Authority may terminate this Contract for Material Breach where the Supplier, by any act or omission, causes material adverse publicity relating to or affecting the Authority or the Contract. This is true whether or not the act or omission in question was done in connection with the performance by the Supplier of its obligations hereunder.

39. NON DISCRIMINATION

39.1 The Supplier shall:

(a) perform its obligations under the Contract in accordance with:

(i) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy,

maternity or otherwise);

(ii) the Authority's equality and diversity policy as given to the Supplier from time to time;

(iii) any other requirements and instructions which the Authority reasonably imposes in connection with any equality obligations imposed on the Authority at any time under applicable equality Law; and

(b) take all necessary steps and inform the Authority of the steps taken to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation).

40. PREMISES

40.1 Where either Party uses the other Party's premises, such Party is liable for all Loss or damage it causes to the premises. Such Party is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

40.2 The Supplier will use the Authority's premises solely for the Contract.

40.3 The Supplier will vacate the Authority's premises upon termination or expiry of the Contract.

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

40.5 While on the Authority's premises, the Supplier will:

(a) ensure the security of the premises;
(b) comply with Authority requirements for the conduct of personnel;
(c) comply with any health and safety measures implemented by the Authority;
(d) comply with any instructions from the Authority on any necessary associated safety measures; and
(e) notify the Authority immediately in the event of any incident occurring on the premises where that incident causes any personal injury or damage to Property which could give rise to personal injury.

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

40.7 All Equipment brought onto the Authority's premises will be at the Supplier's risk. Upon termination or expiry of the Contract, the Supplier will remove such Equipment.

41. EQUIPMENT

41.1 Any Equipment brought onto the premises of the other party will be at the owner's own risk and the other party will have no liability for any Loss of, or damage to, any Equipment.

41.2 Upon termination or expiry of the Contract, the equipment supplying party will remove the Equipment, and any other materials, leaving the premises in a safe and clean condition.

42. SEVERABILITY

42.1 If any part of the Contract becomes invalid, illegal or unenforceable, it will be severed from the Contract and the remaining parts of the Contract or any SOW will be unaffected.

42.2 If any fundamental part of this Contract becomes invalid, the Authority and the Supplier may agree to remedy the invalidity. If the Parties are not able to do so within 20 working days of becoming aware of the invalidity, the Contract will be automatically terminated.

43. EMPLOYER LIABILITY INSURANCE

43.1 The Supplier will have employer's liability insurance of at least £5,000,000 prior to Contract award. Thereafter, Suppliers will need to maintain such further insurances and to the indemnity levels specified by the Authority in the Contract Data or SOW.

44. COMMUNICATION

44.1 Any notices sent in relation to this Contract must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'. The Authority's email address is: commercialcontracts@cqc.org.uk

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

Manner of Delivery	Deemed time of delivery	Proof of Service
Email	9am on the first Working Day after sending	Dispatched in an emailed pdf to the correct email address without any error message

45. RELATIONSHIP

45.1 Neither Party can act as agent of the other or make representations on their behalf.

46. VARIATION

46.1 This Contract may be amended if the Authority notifies the Supplier that it wishes to change the provisions of this Contract (including any variations suggested by the Supplier) and provides the Supplier with full written details of any such proposed change. Both Parties must agree to the variation and a Change Control Notice ("CCN") in the form appended to Schedule 4 must be completed and be signed by both Parties.

46.2 If no agreement is reached by the Parties within (90) Working Days after notification was given, the Authority may either:

(i) agree that the Parties shall continue to perform their obligations under this Contract without the variation; or

(ii) terminate this Contract.

47. NOT USED

48. SUBCONTRACTING

48.1 The Supplier will deliver the services offered and will not solely source staff for others.

48.2 The Supplier will only subcontract with the approval of the Authority. If the Supplier chooses to use Sub-contractors, this will be outlined in any bid along with the percentage of delivery allocated to each Sub-contractor.

48.3 The Supplier will take direct contractual responsibility and full accountability for delivering the services they provide using Sub-contractors.

49. ENVIRONMENTAL REQUIREMENTS

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

49.2 The Supplier must support the Authority in their efforts to work in an environmentally- friendly way, e.g. by helping them engage in practices like recycling or lowering their carbon footprint.

50. TRANSPARENCY AND ACCESS TO RECORDS

50.1 Transparency

50.1.1 In accordance with the government's policy on transparency, the Authority reserves the right to make all or part of the information (including the Contract and any SOW) publicly available (subject to any redactions made at the discretion of the Authority by considering and applying relevant exemptions under the FoIA). Commercially sensitive elements of the contract will be redacted if exempt under the FoIA

50.1.2 The Supplier permits the Authority to publish the full text (excluding commercially sensitive information) of this Contract after considering (at Authority's sole discretion) any representations made by the Supplier regarding the application of any relevant FoIA or EIR exemptions.

50.2 Who can carry out an audit or inspection?

Representatives of the following auditors will have access to the Supplier's records and accounts:

- the Cabinet Office
- the National Health Service
- the Authority
- the National Audit Office
- any auditor appointed by the Audit Commission

50.3 What will happen during the Contract's term

50.4 The Supplier will keep and maintain in accordance with Good Industry Practice and generally accepted accounting principles, full and accurate records and accounts of all of the following:

(i) the operation of the Contract;
(ii) the Services provided under the Contract (including any subcontracts); and
(iii) the amounts paid by the Authority under the Contract.

50.4 What will happen when the Contract ends

50.4.1 The Supplier will provide a completed self-audit certificate to the Authority within 3 months.

50.4.2 The Supplier's records and accounts will be kept until the latest of the following dates:

(i) 3 years after the date of termination or expiry of this Contract; and/or
(ii) another date that may be agreed between the Parties

50.4.3 During the timeframes highlighted in clause 50.4.2, the Supplier will:

a) allow the previously listed auditors to inspect or audit its records;
b) keep the data from the Contract;
c) keep commercial records of:

- the Charges, and any variations to them (actual or proposed)
- costs, including Sub-contractors' costs

d) keep books of accounts for this Contracts;
e) keep MI reports;
f) maintain access to its published accounts and trading entity information;
g) maintain an asset register of all Intellectual Property Rights (IPR); Equipment and facilities (used, acquired, developed) under this Contract;
h) maintain proof of its compliance with obligations under Data Protection, and Transparency and Security regulations; and
i) maintain records of its delivery performance under each Contract, including that of Sub-contractors.

50.5 What will happen during an audit or inspection

50.5.1 The auditor will use reasonable endeavours to ensure that the conduct of the audit does not:

(a) unreasonably disrupt the Supplier; and/or
(b) delay the provision of Services under any Contract or SOWs.

50.5.2 Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to:

a) provide information without unreasonable delay
b) provide all information within scope
c) give auditors access to:
    - each site controlled by the Supplier
    - any Equipment used to provide the Services
    - the Supplier's staff

50.5.3 An auditor will be able to review, inspect and examine the Supplier's records and accounts associated with this Contracts. This is to:

(a) verify the accuracy of:
- the Charges (and proposed or actual variations to them in accordance with this Contract);
- the costs of the Supplier (including any Sub-contractor's costs);

(b) review the integrity, Confidentiality and security of the Personal Data and Authority Data held or used by the Supplier;

(c) review any books of accounts kept by the Supplier in connection with the provision of the Services, for the purposes of auditing the Charges and Management Charges under the Contract;

(d) review any other aspect of the delivery of the Services including to review compliance with any legislation;

(e) carry out an examination following Section 6 (1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(f) review any internal contract management accounts kept by the Supplier in connection with this Contract;

(g) review any records relating to the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records; and

(h) inspect the Authority's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Authority's assets are secure and that any asset register is up to date.

50.5.4 The Supplier will reimburse Authority's reasonable costs incurred in relation to the audit or inspection, if it reveals that the Supplier has committed a material Default. The Authority will reimburse the Suppliers reasonable costs incurred in relation to the audit or inspection, if it reveals that the Supplier has not committed a material Default.

50.5.5 Each Party is responsible for covering all other costs that they may incur from their compliance with the obligations of this Contract

51. Rights of Third Parties

A person who is not Party to this Contract has no right to enforce any term of this Contract under the Contracts (Rights of Third Parties) Act 1999.

52. Law and jurisdiction

This Contract will be governed by the Laws of England and Wales. Each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

53. Defined Terms

'Application'	The response submitted by the Supplier to the Invitation to Tender
'Background IPRs'	For each Party: • IPRs owned by that Party before the date of this Call-Out Contract, including IPRs

	contained in any of the Party's know-how, documentation, processes and procedures; • IPRs created by the Party independently of this Call-Out Contract; and/or • For the Authority, Crown Copyright which is not available to the Supplier otherwise than under this Call-Out Contract; but excluding IPRs owned by that Party subsisting in Authority Software or Supplier Software
'Authority Background IPRs'	Background IPRs of the Authority
'Authority's Confidential Information'	All Authority Data and any information that relates to the business, affairs, developments, trade secrets, know-how, personnel, and Suppliers of the Authority, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above Any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential')
'Authority Data'	Data that is owned or managed by the Authority, including Personal Data gathered for user research, e.g. recordings of user research sessions and lists of user research participants
'Authority Software'	Software owned by or licensed to the Authority (other than under or pursuant to this Agreement), which is or will be used by the Supplier for the purposes of providing the Services
'Contract'	This legally binding agreement for the provision of Services made between the Authority and the Supplier This may include the key information summary, Contract Data, requirements, Supplier's response, Statement of Work (SOW), Contract Change Notice (CNN) and terms and conditions as set out in the Contract Data
'Charges'	The prices (excluding any applicable VAT), payable to the Supplier by the Authority under the Contract, as set out in the applicable SOW(s), in consideration of the full and proper performance by the Supplier of the Supplier's obligations under the Contract and the specific obligations in the applicable SOW.
'Commercially Sensitive Information'	Information, which the Authority has been notified about, (before the start date of the Contract) with full details of why the Information is deemed to be commercially sensitive
'Comparable Supply'	The supply of services to another customer of the Supplier that are the same or similar to any of the Services
'Confidential Information'	The Authority's Confidential Information or the Supplier's Confidential Information, which may include (but is not limited to):

	• any information that relates to the business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • any other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential'
'Control'	Control as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly
'Crown'	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf
"Data Controller, Data Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer"	shall each have the same meaning given in the GDPR;
"Data Loss Event"	Means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Protection Legislation"	Means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii) the DPA 2018 (subject to Royal Assent) to the extent that it relates to the processing of Personal Data and privacy; (iii) all applicable Law about the processing of Personal Data and privacy.
"Data Protection Impact Assessment"	Means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
"Data Subject Access Request"	Means a request made by or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access his or her Personal Data.
'Default'	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)

	• other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract
'Deliverable'	A tangible work product, professional service, outcome or related material or item that is to be achieved or delivered to the Authority by the Supplier as part of the Services as defined in the Contract Data and all subsequent Statement of Work
"DPA"	Means the Data Protection Act 2018 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such legislation;
'Equipment'	The Supplier's or Authority's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier or Authority in the performance of its obligations under this Contract.
'FoIA'	The Freedom of Information Act 2000 and any subordinate legislation made under the Act occasionally together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation
"GDPR"	means the General Data Protection Regulation (*Regulation (EU) 2016/679*)
'Good Industry Practice'	Standards and procedures conforming to the Law and the application of skill, care and foresight which would be expected from a person or body who has previously been engaged in a similar type of undertaking under similar circumstances. The person or body must adhere to the technology code of practice (https://www.gov.uk/service-manual/technology/code-of-practice.html) and the government service design manual (https://www.gov.uk/service-manual)
'Group'	A company plus any subsidiary or holding company. 'Holding company' and 'Subsidiary' are defined in section 1159 of the Companies Act 2006
'Group of Economic Operators'	A partnership or consortium not (yet) operating through a separate legal entity.
'Holding Company'	As described in section 1159 and Schedule 6 of the Companies Act 2006
'Information'	As described under section 84 of the Freedom of Information Act 2000, as amended from time to time
'Insolvency Event'	may be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator

	• an unresolved statutory demand • a Schedule A1 moratorium
'Intellectual Property Rights' or 'IPR'	means: a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, service marks, logos, database rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, design rights (whether registerable or otherwise), Know-How, trade secrets and moral rights and other similar rights or obligations whether registerable or not; b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and c) all other rights whether registerable or not having equivalent or similar effect in any country or jurisdiction (including but not limited to the United Kingdom) and the right to sue for passing off.
"Key Performance Indicators"	means the key performance indicators listed in the Schedule 11 and a Key Performance Indicator ("KPI") shall mean any one of them.
'Key Staff'	Means the Supplier Staff if named in the SOW as such
'KPI Target'	The acceptable performance level for a key performance indicator (KPI)
'Law'	Means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply.
"LED"	Means Law Enforcement Directive *(Directive (EU) 2016/680)*.
'Loss'	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and 'Losses' will be interpreted accordingly.
'Malicious Software'	Any software program or code intended to destroy, or cause any undesired effects. It could be introduced wilfully, negligently or without the Supplier having knowledge of its existence.
'Material Breach (Contract)'	A single serious breach of or persistent failure to perform as required in the Contract Or a breach of any of the following Clauses: • Subcontracting

	• Non-Discrimination • Conflicts of Interest • Warranties and Representations • Prevention of Bribery and Corruption • Safeguarding against Fraud • Data Protection and Disclosure • Intellectual Property Rights and Indemnity • Confidentiality • Official Secrets Act • Audit
'Contract Data'	Part A of this contract which contains the important information about this Contract.
'Party'	The Authority and the Supplier.
'Personal Data'	Personal data (as defined in the Data Protection Legislation) which is Processed by the Supplier or any Sub-contractor on behalf of the Authority or a Central Government Body pursuant to or in connection with this Contract.
"Processing"	Has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted accordingly;
'Prohibited Act'	To directly or indirectly offer, promise or give any person working for or engaged by a Authority a financial or other advantage to: • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: o under the Bribery Act 2010 o under legislation creating offences concerning Fraud o at common Law concerning Fraud o committing or attempting or conspiring to commit Fraud
'Project-Specific IPRs'	• Intellectual Property Rights in items, including Deliverables, created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Contract and updates and amendments of these items including (but not limited to) database schema; and/or • Intellectual Property Rights arising as a result of the performance of the Supplier's obligations under this Contract; but not including the Supplier Background IPRs

'Property'	The property, other than real property and IPR, issued or made available to the Supplier by the Authority in connection with a Contract
"Protective Measures"	Means appropriate technical and organisational measures which include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
'Regulations'	The Public Contracts Regulations 2015 (at http://www.legislation.gov.uk/uksi/2015/102/contents/made) and the Public Contracts (Scotland) Regulations 2012 (at http://www.legislation.gov.uk/ssi/2012/88/made)
'Regulatory Bodies'	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Contract.
"Regulator Correspondence "	means any correspondence from the Information Commissioner's Office, or any successor body, in relation to the Processing of Personal Data under this Contract.
'Request for Information'	A request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations
'Services'	ESB Application Support and Development to be provided by the Supplier under this Contract as further outlined in the Specification.
'Specific Change in Law'	A change in the Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply
'Specification	A statement issued by the Authority detailing its Services requirements issued in the Contract
'Statement of Work' (SOW)	The document outlining the agreed body of works to be undertaken as part of the Contract between the Authority and the Supplier. This may include (but is not limited to) the Specification, the Deliverable(s), the completion dates, the charging method. Multiple SOWs can apply to a Contract.
'Sub-contractor'	Each of the Supplier's Sub-contractors or any person engaged by the Supplier in connection with the provision of the digital services as may be permitted by this Contract.
"Sub-processor"	means any third Party appointed to process Personal Data on behalf of the Supplier related to this Contract;
'Supplier Background IPRs'	Background IPRs of the Supplier.
'Supplier Software'	Software which is proprietary to the Supplier and which is or will be used by the Supplier for the purposes of providing the Services.

'Supplier Staff'	Means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Sub-Contractor (including employees) engaged in the performance of its obligations under this Contract.
"Variation"	Means a variation to the Specification, SOW, the Price or any terms or conditions of the Contract.
'Working Day'	Any day other than a Saturday, Sunday or public holiday in England and Wales, from 9am to 5pm unless otherwise agreed with the Authority and the Supplier in the Contract.