Crown Commercial Service

Contract

Contents

Part A - Order Form

Contract reference:	CSR/105
Contract title:	CSL Support and Maintenance
Contract description:	The provision of website support and maintenance services to ensure the effective upkeep and operation of the Civil Service Learning website
Contract value:	Initial term total value: £47,083 Optional 6 month extension total value: £60,113
Charging method:	By invoice
Purchase order number:	TBC

This Order Form is issued in accordance with the referenced G-Cloud 11 Framework Agreement (RM1557.11) terms.

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

From: the Buyer	Cabinet Office on behalf of Civil Service Human Resourcing Buyer's main address: 70 Whitehall Westminster London SW1A 2AS
To: the Supplier	Axis12 Ltd 0845 519 5465 Supplier's address: Unit 14, The Ivories, 6-18 Northampton St London N1 2HY Company number: 07215135
Together: the 'Parties'	

Principal contact details

For the Buyer:	Title: Commercial Lead Name: [REDACTED] Email: [REDACTED]

	Phone: [REDACTED]
For the Supplier:	Title: Director Name: [REDACTED] Email: [REDACTED] Phone: [REDACTED]

Contract term

Start date:	This Contract starts on 25th January 2020
Contract period:	Initial Term: 25th January 2020 to 24th July 2020 Optional 6 month extension: 25th July 2020 – 24th January 2021
Ending (termination):	The notice period needed for Ending the Contract is at least 90 Working Days from the date of written notice for undisputed sums or at least 30 days from the date of written notice for Ending without cause.

Buyer contractual details

This Order is for the Services outlined below.

G-Cloud lot	This Call-Off Contract is for the provision of Services under: Lot 3 - Cloud support
Services required:	The Services to be provided by the Supplier are outlined below on Schedule 1 - Services.
Location:	The Services will be delivered to: Civil Service Learning 2 Marsham Street Westminster London SW1P 4DF
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed £1,000,000. The annual total liability for Buyer Data defaults will not exceed £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Contract Term (whichever is the greater). The annual total liability for all other defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Contract Term (whichever is the greater).
Insurance:	The insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Contract

	● Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● Employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	A Party may End this Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 15 consecutive days.
Audit:	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Contract to enable the Buyer to carry out audits. 7.4 The Supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the: ● operation of the Contract ● Services provided under the Contract 7.6 The Supplier's records and accounts will be kept until the latest of the following dates: ● 7 years after the date of Ending or expiry of this Contract ● another date agreed between the Parties 7.7 During the timeframes highlighted in clause 7.6, the Supplier will maintain: ● commercial records of the Charges and costs (including Subcontractors' costs) and any variations to them, including proposed variations ● books of accounts for this Contract ● MI Reports ● access to its published accounts and trading entity information ● proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Contract ● records of its delivery performance under each Contract, including that of its Subcontractors What will happen during an audit or inspection 7.8 The Buyer will use reasonable endeavours to ensure that the Audit does not unreasonably disrupt the Supplier, but the Supplier accepts that control over the conduct of Audits carried out by the auditors is outside of the Buyer's control. 7.9 Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to: ● provide audit information without delay ● provide all audit information within scope and give auditors access to Supplier Staff

	7.10 The Supplier will allow the representatives of Buyer receiving Services, the Controller and Auditor General and their staff, any appointed representatives of the National Audit Office, HM Treasury, the Cabinet Office and any successors or assigns of the above access to the records, documents, and account information referred to in clause 7.7 (including at the Supplier's premises), as may be required by them, and subject to reasonable and appropriate confidentiality undertakings, to verify and review: ● the accuracy of Charges (and proposed or actual variations to them under this Contract ● 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 only ● the integrity, Confidentiality and security of the Buyers Personal Data and the Buyer Data held or used by the Supplier ● any other aspect of the delivery of the Services including to review compliance with any legislation ● the accuracy and completeness of any MI delivered or required ● any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records ● the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date Costs of conducting audits or inspections 7.11 The Supplier will reimburse the Buyer its reasonable Audit costs if it reveals: ● a Material Breach 7.12 the Buyer can End this Contract for Material Breach if the event in clause 7.11 applies. 7.13 Each Party is responsible for covering all their own other costs incurred from their compliance with the Audit obligations.

Buyer's responsibilities:	The Buyer is responsible for: • Providing the Supplier with all necessary cooperation in relation to the agreement and all necessary access to such information as may be required by the Supplier in order to render the Services, including but not limited to Buyer Data, specification information, security access information and software interfaces to the website • Comply with all applicable laws and regulations with respect to its activities under the agreement • Carry out all Buyer responsibilities set out in the agreement or in any of the schedules included within the Terms and Conditions (attached separately) in a timely and efficient manner. In the event of any delays in the Buyer's provision of such assistance as agreed by the parties, the Supplier may adjust any timetable or formerly agreed delivery schedule as reasonably necessary

Contract charges and payment

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

Payment method:	The payment method for this Contract is by BACS
Payment profile:	The payment profile for this Contract is monthly in arrears.
Invoice details:	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to: [REDACTED]
Invoice information required – for example purchase order, project reference:	All invoices must include: ● PO number ● Contract title and reference ● Invoice amount ● Date ● Breakdown of invoice e.g. number of project days as proposed in pricing and day rate.
Invoice frequency:	Invoice will be sent to the Buyer monthly.
Contract charges:	The breakdown of the Charges are detailed in Schedule 2.

1. Formation of contract

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

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

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

1.4 In cases of any ambiguity or conflict the terms and conditions of the Contract and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of Services and agreed to provide the Services under the Contract terms.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:	[REDACTED]	[REDACTED]
Title:	[REDACTED]	[REDACTED]
Signature:	X [REDACTED]	X [REDACTED]
Date:	[REDACTED]	[REDACTED]

Schedule 1 – Services

Introduction and background

The Civil Service Learning (CSL) website is an internal-facing transactional service that supports and administers learning for the Civil Service. The website is used by approximately 415,000 users and includes mandatory and non-mandatory training in the form of e-learning and face-to-face training.

The CSL website is fully owned by the Civil Service and hosted on Rackspace. The website is built from Moodle and Drupal. The CSHR Digital and Analysis team work to agile methodologies and will expect the Supplier maintaining the CSL website to be experts in agile delivery and to participate in agile ceremonies. The Supplier will also be expected to collaborate with CSL to ensure the CSL website is maintained to a high standard, in accordance with agreed SLAs and OLAs as stated in Annex A, and developed according to a user-focused approach.

Flexibility in service provision must be available, in particular the ability to increase or decrease the Service provision as required to provide scalability. For example, it should be possible to pay less if fewer users are accessing the system or if data holdings are less than expected. In their response, Suppliers should provide options to downsize the Service and state bandings for tiered service provision based on usage and volume of data holdings.

Standard Cabinet Office payment terms will apply.

All staff employed on the project on behalf of the Supplier should be willing to undergo BPSS security clearance as a minimum as well as CTC if accessing 2 Marsham Street. Additional Security Clearance will be mandatory for any staff accessing bulk data.

The Supplier must possess or be willing to achieve ISO 27001:2013 certification and Cyber Essential Plus certification within an agreed (with the Buyer) timescale.

Scope

The provision of maintenance and support services for the CSL website until the new Learning Platform for Government (LPG) is ready to go live in 2020/2021, and facilitating the transition to the new platform, migrating historic user and management information data between the CSL and LPG systems.

Scope of support includes the following.

- Support and maintenance of the Drupal Portal site
- Support and maintenance of the Drupal Coaching site
- Support and maintenance of the PHP Reporting application
- Support and maintenance of the Moodle site
- Support and maintenance of Production Rackspace environment
- Support and maintenance of Non-production Axis12 environment

The specification of current servers and systems is set out in Annex B any development of these systems, will be need to be agreed outside the scope of these services and the rate card will apply to costs.

The contract will commence in January 2020 for a minimum of 6 months with an optional to extend an additional 6 months, up to a maximum of 12 months.

The services will be delivered at both the Supplier's premises and 2 Marsham Street, Westminster, London, SW1P 4DF. The Supplier will be required to travel to London (if not based in London). Travel and subsistence will not be provided.

Delivery of maintenance and support services

Maintenance and support services will be delivered in accordance with the Axis12 proposal and clarifications set out in Annex C and D and the following requirements.

User support

Second-line support for the website., including a response to, investigate and resolve issues and problems received from first-line support (helpdesk) or the CSL Digital Team between 9am to 5.30pm Monday to Friday (excluding bank holidays). To raise and action any development requirements when third-line development support is required.

To support the administration of the CSL website in collaboration with CSL Digital Team. When first-line support is unable to assist, the Supplier may be required to provide front-end support to third-party training providers, including: publishing new content, updating sub-menus and page elements such as videos and headings. (These changes will be funded by the training provider, who has requested the change, and will not constitute part of this contract.)

Maintenance of servers and systems

All systems to be maintained to a consistently high standard, in line with the SLAs and OLAs as stated in Annex A. The Supplier should ensure that there is sufficient team resource to deliver the platform in accordance with the SLAs/OLAs.

The Supplier will be expected to carry out the following tasks under maintenance. However this list is not exhaustive and, where tasks are required in order to meet the SLAs and OLAs, these should also be actioned under maintenance.

- bug and issue investigation and resolution.
- problem identification, management and resolution.
- general maintenance and small change controls.
- functionality and quality assurance testing.
- Solutions Architect support.
- ongoing patches and updates to Moodle.
- ongoing patches and updates to Drupal.
- ongoing patches and updates to supporting services (i.e. Apache).
- monitoring and management of server load and disk space for optimal performance.
- custom script optimisation.
- monitoring, analysing and resolving issues with load capacity in response to load testing and live performance.
- monitoring and responding to alerts.
- ad hoc web server and database server configuration adjustment to optimise website running.

- CRON changes & scripting for ongoing development & reporting.
- staging and development website setup; maintenance of staging and development platforms; establish and maintain the staging environment as an effective mirror of live (rsync site files, copy databases, vhost changes etc).
- general Developer help/interaction for CSL server for development changes.
- raise and manage tickets wither server provider (high load, general, SAN changes etc).
- review and analyse error logs in order to ensure optimal performance (PHP, MySQL, Apache, etc.)
- review, monitor, diagnose and resolve issues affecting server and/or website when slow running is reported.
- promptly fix and restore the website when outages occur. See response and resolution times, outlined in SLAs/OLAs as stated in Annex A.
- respond to website monitoring alerts promptly and in line with agreed SLAs/OLAs as stated in Annex A.
- renew and manage SSL certificates.
- manage and monitor load balancer, including configuration management and implementation of adjustments (SSL & VIP's etc).

Development standards

The Supplier will be required to develop and maintain the platform in accordance with the Digital Service Standard at a https://www.gov.uk/service-manual/service-standard and will be responsible for ensuring that deployments are consistent across environments, testing is automated and deployment is low-risk. Code will only be deployed when there is good reason for knowing it works.

Security requirements

The Supplier is to identify and mitigate security risks.

Security governance

To improve the effective security management of the Service. The Supplier will be expected to provide robust management/reporting of residual risks, improvements in the reporting of operational security matters and the management of security incidents.

Technical security

Protective monitoring

An effective protective monitoring regime must be in place at all times and produce sufficient evidence in the form of logs and other documents to the Buyer to confirm this. The Supplier should maintain and provide monthly intrusion detection system reports tracking all incidents, their status, threat level and any mitigations to prevent further threats.

Patching and support

The Supplier will be expected to ensure that all platforms are up-to-date with patches and upgrades and all versions of products remain supported.

Data protection

The Supplier will be expected to ensure the Service is compliant with the new GDPR legislation.

Personnel vetting requirements

As a minimum, all staff must comply with the Baseline Personnel Security Standard. All Supplier staff must complete the personnel security controls that are described in the Baseline Personnel Security Standard before commencing work.

Supplier staff, who will have access to bulk live data (classified as Official Sensitive data), must be willing to undergo an elevated clearance level (SC).

Supplier staff, who will be working in 2 Marsham Street, will need to undergo a Counter Terrorism Check (CTC).

Designing and managing secure solutions

The Supplier will be expected to design secure solutions in accordance with the NCSC Security Design Principles at https://www.ncsc.gov.uk/collection/cyber-security-design-principles For example implementing segmented and layered network architectures and comprehensive protective monitoring solutions.

The Supplier must demonstrate competencies and have a proven ability for implementing solution(s) which mitigate the security risks for an internet facing web service. As part of evidencing this ability, a risk assessment needs to be produced, which describes the procedural, technical and physical controls implemented, and how any security vulnerabilities have been mitigated.

The Supplier shall demonstrate how they are monitoring vendors and national vulnerability databases. They should also be able to clearly explain how this information is used to inform the developing design process to ensure the appropriate security controls are put in place to mitigate the risk.

The Supplier shall provide a risk assessment for the Service to ensure that the Service is compliant with Protecting Bulk Personal Data - https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data and Cloud Security Principles - https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

This assessment will be reviewed on an annual basis or if there is a major incident or change to infrastructure, processes and procedures.

Certification requirements

The Supplier's solution shall be ISO27001:2013 certified and Cyber Essential Plus or be willing to obtain this certification within an agreed timescale.

Patching and penetration testing

The Supplier must proactively monitor Supplier vulnerability websites and demonstrate the ability to ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the Cloud Security Principles. The Supplier must undertake the following security assurance activities and expense in order to demonstrate that the people, process, technical and physical controls have been delivered in an effective way:

- Penetration testing to be carried out by certified Crest or Check Supplier.
- Penetration testing of the production environment before the first release to that environment.
- An annual IT Health Check (scope to be agreed with the Buyer) and where there is a significant change to infrastructure/service.
- After receiving IT health check report. The full report must be shared with the Buyer and the Supplier must produce a remediation plan to agreed timescales which will be managed through a security working group.

Protective monitoring

The Supplier must ensure an effective protective monitoring regime is in place at all times and produce sufficient evidence in the form of logs and other documents to the Buyer to confirm this.

The Supplier should:

- Provide operational security management reports.
- Engage with the Buyer incident management process.
- Demonstrate the ability to deliver protective monitoring across the supply chain.
- Incorporate National Cyber Security Centre (NCSC) guidance on how to design a security operations centre (SOC).

Data processing, storage, management and destruction

The Supplier and Buyer recognise the need for the Buyer Data to be safeguarded under the Data Protection Act (DPA). To that end, at all times, the Supplier must be able to state to the Buyer the physical locations within the European Economic Area where the Buyer Data may be stored, processed and managed.

The Supplier shall ensure that the subcontractors do not store, process or transmit Buyer Data outside the European Economic Area and the Supplier shall agree any change in location of data storage, processing and administration with the Buyer in advance and such agreement may be subject to conditions.

The Supplier must securely erase any or all Buyer Data held by the Supplier, when requested to do so by the Buyer, and securely destroy all media that has held Buyer Data at the end of life of that media. When destroying media, the Supplier must ensure that it is destroyed in accordance with the Buyer's requirements and, in the absence of any such requirements, in accordance with Good Industry Practice.

Business continuity and disaster recovery planning

The Supplier must create, maintain and test business continuity and disaster recovery plan(s) and ensure that the Buyer is aware of these plans and informed when changes are made to existing plans.

Governance and delivery

The project will be run using the agile methodology, which is mandated by Government Digital Service, and in accordance with the commercial contract and Statement of Work (SoW). Progress will be monitored at daily stand ups and work will be managed through sprint cycles. This approach will allow the user needs to be re-prioritised on a regular basis to ensure the delivery of the essential

elements of the platform, while ensuring the agreed outcomes are achieved. Some planned development work is expected, however the full scope remains to be agreed.

Throughout the life of the contract, we will have regular contract and security management meetings every 4 weeks. These meetings will enable us to work together to:

- track, review and plan the delivery and achievement of the milestones.
- review performance, ensuring that contractual KPIs/SLAs are being achieved and will instigate remedial action if not.
- drive the realisation of contractual obligations.
- ensure the project is delivering benefits that will be evidenced through data.
- actively manage security risk and mitigation with Suppliers as part of our Security Governance Framework (including risks, breaches and changes to infrastructure and processes) to ensure Suppliers are compliant with contracts and are actively managing and reporting risk.
- the Supplier must be willing to fully engage with external and internal scrutiny including audits and reviews.
- we require the Supplier to ensure continuous improvement is embedded across their processes.
- the Supplier should be prepared to fully engage in continuous improvement initiatives that are initiated by the Buyer and its third-party Suppliers.

Exit plan

An exit plan will be agreed, in conjunction with the Buyer and relevant Suppliers, to enable the successful transfer of deliverables to the new Supplier. The exit plan is expected to ensure that the Supplier has all the code and documentation required to support and continuously develop the Service. The Supplier will update this plan whenever there are material changes to the Service. A Statement of Work (SoW) may be agreed between the Buyer and the Suppliers to specifically cover the exit plan.

The initial high-level exit plan will be submitted within 3 months of the contract award. The final exit plan should be agreed within 3 months before the contract ends.

Service levels and performance

The Buyer will measure the quality of the Supplier's delivery in accordance with the SLAs/OLAs (see Annex A). The criteria for assessing quality are expected to include:

- Service availability.
- Issue resolution and response times.
- In-hours support (Monday to Friday between 9am and 5.30pm).
- Named single point of contact for all queries without SPOF.
- All Supplier staff are to be security cleared and UK based.
- Data hosted in the EEA.

- Cyber Essentials Plus certification and ISO 27001 compliance.
- Compliance with NCSC guidelines.
- Compliance with Digital Service Standard.
- Compliance with NCSC cloud principles.
- Deployment of critical and standard changes.
- Quality of changes and warranties.
- A minimum of 3 working days' notice of any scheduled downtime.
- Manage the hosting provider and ensure they adhere to and are operating within agreed service levels.
- Staff retention and backfilling posts.

Annex

Annex A: SLAs and OLAs

ID	SLA
1	The Supplier will proactively monitor server load and disk space and ensure optimal site running between the hours of 9am and 5.30pm. If issues are identified with site performance, then the Supplier will make the Buyer aware of these at the earliest opportunity and take appropriate action in agreement with the Buyer to restore optimal site performance.
2	Triage, respond to and resolve all tickets raised to second-line support by phone or email, according to prioritisation: Critical (2 hours), High (4 hours), Medium (2 days) and Low (5 days) priority.
3	The Supplier must respond to and resolve site-wide incidents, or incidents affecting business critical areas of the website. Critical incidents should be reported with 30 minutes and resolved within 2 hours.
4	The Supplier will ensure that the website is available 99.95% of time (24/7) and will provide monthly reporting to demonstrate website uptime and availability.
5	Where downtime or site performance is likely to be impacted, the Supplier should ensure that the Buyer is made aware of the impact a minimum of 3 working days before a change is to be implemented. All changes that could potentially impact website performance must take place out-of-hours and in agreement with the Buyer.
6	The Supplier will run an annual pentest and retest with a CHECK or Crest accredited Supplier at their own expense and share the results in full so that we can manage the system's ongoing security. The Supplier will be responsible for fixing security issues identified in pentesting within 6 weeks of the test. A retest will be required within 1 month of the changes being implemented.
7	The platform/system will scale to provide a stable experience to all users, including at peak times when we would expect a maximum of 2000 concurrent users.
8	The Supplier will ensure that all page response times are .1 second or below.
9	The Supplier will agree a suitable sprint velocity with the Buyer. Sprints will be delivered at a fixed cost on the assumption that the level of work committed to per sprint will support consistent iterative delivery and exceed a minimum delivery of 70%. Work will only be considered to be delivered once it has been released to the live environment and in use for a minimum of 10

	working days without issues arising.
10	The Supplier should ensure that requests for change in personnel from the Buyer are responded to and implemented with 3 days so that we can maintain the integrity and coherence of the delivery team.

ID	OLA	
1	The Supplier has clearly documented Business Continuity plans, including out of hours arrangements.	The Supplier will be asked to supply business continuity documentation and update on the status of business continuity plans as part of contract management. *Contract management meeting, update on changes and testing.
2	The Supplier has clearly documented Disaster Recovery arrangements, including out of hours support.	The Supplier will be asked to supply disaster recovery documentation and update on the status of disaster recovery plans as part of ongoing contract management. *Contract management meeting, update on changes and testing.
3	The Supplier will maintain a security risk register to be shared with us and provide a named person to attend the Security Working Group.	The Supplier will be asked to supply a security risk register and update on security and data risk as part of ongoing contract management. *Contract management meeting, update on risks and mitigations.
4	The Supplier will maintain and share a finance tracker showing all invoicing amounts related to specific Statements of Work and Purchase order numbers and rate of spend.	The Supplier will be asked to supply a finance tracker and update on the financial spend as part of ongoing contract management.

		*Contract management meeting, update on spend and costs.

Annex B. Current specification

- Web server 96Gb RAM, 2 x Hex Core Xeon Processors, 2 x 300Gb Hard Disks
- Web server 96Gb RAM, 2 x Hex Core Xeon Processors, 2 x 300Gb Hard Disks
- Web server 96Gb RAM, 2 x Hex Core Xeon Processors, 2 x 300Gb Hard Disks
- Web server 96Gb RAM, 2 x Hex Core Xeon Processors, 2 x 300Gb Hard Disks
- Staging server - Web server 96Gb RAM, 2 x Hex Core Xeon Processors, 2 x 600Gb Hard Disks
- Database Server – 64Gb RAM, 2 x Hex Core Xeon processors
- Database Server – 64Gb RAM, 2 x Hex Core Xeon processors
- Firewall – 450mbps throughput
- Load Balancer
- SAN Fibre based storage area network – 150Gb of database storage, 900Gb of Website storage
- Off-site backup storage – daily backups retained for 4 weeks.

Annex C. Axis 12 Proposal for the extension of support and maintenance of the Civil Service Learning website [REDACTED]

Annex D. Axis12 Clarification of proposed services to be delivered

Maintenance of the hosting infrastructure including monitoring; troubleshooting; applying OS patches, including five (5) days development work.

2nd line support of the Drupal Portal; Drupal Coaching site; PHP Reporting application and Moodle site whereby 2nd line support is defined as 'Non-technical operational tasks where documented procedures have been provided; application configuration; content changes; application changes that do not require technical design and/or development activities'.

3rd line support, defined as work that requires technical design and/or development, is not covered within the 5 day 'support and maintenance' allocation, and is requested under separate purchse order.

In the event that NCC testing is required during the period, the sAxis12 have allowed for a set amount of time to support their testing efforts (making environments accessible to them; providing necessary pre-test information etc), however Axis12 have not allowed for any time to conduct post-test remedial actions as the quantity of this work will not be known until (and/or if) the tests are carried out. These activities may include: updates to the Rackspace infrastructure; updates to application libraries and modules. It is very difficult to say what actions may be required, but as an indication, when the tasks were previously conducted. Axis12 believe there was about 5 days of remedial actions required from their side.

SLAs, warranty and governance compliance to be carried over as per current contract.

We are using G-Cloud call-off terms and conditions as per current contract and termination clauses are included.

Schedule 2 - Contract charges

The prices in this schedule are fixed for the duration of the contract, unless otherwise stated.

Initial term costs

Item description	Charge
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
Initial term total:	**£47,083.00**

Optional 6 month extension charges

Item description	Charge
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
6 month extension total	**£60,113.00**

Rate card 2020

Role	Day rate
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Part B - Terms and conditions

1. Contract start date and length

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

1.2 This Contract will expire on the Expiry Date in the Order Form.

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.49 to 8.51 (Publicity and branding)
- 8.52 to 8.54 (Equality and diversity)

- 8.57 to 8.58 (data protection)
- 8.62 to 8.63 (Severability)
- 8.64 to 8.77 (Managing disputes and Mediation)
- 8.78 to 8.86 (Confidentiality)
- 8.87 to 8.88 (Waiver and cumulative remedies)
- 8.89 to 8.99 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

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

- a reference to the 'Framework Agreement' will be a reference to the 'Contract'
- a reference to 'CCS' will be a reference to 'the Buyer'
- a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Contract

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

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

3. Supply of services

3.1 The Supplier agrees to supply the Services and any Additional Services under the terms of the Contract and the Supplier's Application.

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

4. Supplier staff

4.1 The Supplier Staff must:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- complete any necessary Supplier Staff vetting as specified by the Buyer

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

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent

experience and qualifications to the substituted staff member.

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

4.5 The Buyer may End this Contract for Material Breach if the Supplier is delivering the Services Inside IR35.

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

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

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

5. Due diligence

5.1 Both Parties agree that when entering into a Contract they:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Contract terms
- have raised all due diligence questions before signing the Contract
- have entered into the Contract relying on its own due diligence

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Contract charges

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

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

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

7.4 If specified in the Order Form, the Supplier will accept payment for Services by the

Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

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

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

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

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

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

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

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

7.12 Due to the nature of Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

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

- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies.

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

- a broker's verification of insurance
- receipts for the insurance premium
- evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under this Contract and the Supplier will:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances
- hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

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

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

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

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

10. Confidentiality

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

11. Intellectual Property Rights

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

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-

free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.

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

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

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

- rights granted to the Buyer under this Contract
- Supplier's performance of the Services
- use by the Buyer of the Services

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

- modify the relevant part of the Services without reducing its functionality or performance
- substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
- buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

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

- the use of data supplied by the Buyer which the Supplier isn't required to verify under this Contract
- other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

- comply with the Buyer's written instructions and this Contract when Processing Buyer Personal Data
- only Process the Buyer Personal Data as necessary for the provision of the Services or as required by Law or any Regulatory Body
- take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

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

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- providing the Buyer with any information requested by the Data Subject

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

13. Buyer data

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

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

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

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

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

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

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/collection/risk-management-collection
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementin-security-principles

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

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

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

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

14. Standards and quality

14.1 The Supplier will comply with any standards in this Contract and the Order Form.

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

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

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

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

15. Open source

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

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

16. Security

16.1 If requested to do so by the Buyer, before entering into this Contract the Supplier will, within 15 Working Days of the date of this Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

17. Guarantee

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

- an executed Guarantee in the form at Schedule 5
- a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Contract

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

18.2 The Parties agree that the:

- Buyer's right to End the Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

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

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

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- any fraud

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

- the other Party commits a Material Breach of any term of this Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
- an Insolvency Event of the other Party happens
- the other Party ceases or threatens to cease to carry on the whole or any material part of its business

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

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

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

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

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

19.4 Ending or expiry of this Contract will not affect:

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability)
- any other provision of this Contract which expressly or by implication is in force even if it Ends or expires

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

- return all Buyer Data including all copies of Buyer software, code and any other

software licensed by the Buyer to the Supplier under it

- return any materials created by the Supplier under this Contract if the IPRs are owned by the Buyer
- stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- work with the Buyer on any ongoing work
- return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

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

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

20. Notices

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

Manner of delivery	**Deemed time of delivery**	**Proof of service**
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error message

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

21. Exit plan

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

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

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

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer

or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

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

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

- the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- it enables the Buyer to meet its obligations under the Technology Code Of Practice

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

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

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

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

- data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
- other information reasonably requested by the Buyer

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

Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

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

23. Force majeure

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

24. Liability

24.1 Each Party's Yearly total liability for defaults under or in connection with this Contract (whether expressed as an indemnity or otherwise) will be set as follows:

- Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

25. Premises

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

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Contract.

25.3 The Supplier will vacate the Buyer's premises when the Contract Ends or expires.

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

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

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health

and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer

- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

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

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

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

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

- its failure to comply with the provisions of this clause
- any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

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

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

30. Additional services

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

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

31. Collaboration

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

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

- work proactively and in good faith with each of the Buyer's contractors
- co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and Services

32. Variation process

32.1 The Buyer can request in writing a change to this Contract if it isn't a material change to this Contract. Once implemented, it is called a Variation.

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

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.57 and 8.58 of the Framework Agreement are incorporated into this Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.57 and 8.58 are reproduced in this Contract document at Schedule 7

Schedule 3 - Collaboration agreement

Intentionally not used

Schedule 4 - Alternative clauses

Intentionally not used

Schedule 5 - Guarantee

Intentionally not used

Schedule 6 - Glossary and interpretations

In this Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the Services that are in the scope of the services offered which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Contract.
Buyer Representative	The representative appointed by the Buyer under this Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Contract	This Contract entered into for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the terms and conditions, the schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, personal data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above

	● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: i) (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to Processing of personal data and privacy; iii) (iii) all applicable Law about the Processing of personal data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner .
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Contract The Supplier is liable to the Buyer.
Deliverable(s)	The Services the Buyer contracts the Supplier to provide under this Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi
Expiry Date	The expiry date of this Contract in the Order Form.
Force Majeure	A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The Government's preferred method of purchasing and payment for low value goods or services https://www.gov.uk/government/publications/government-procurement-card--2.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK Government Guidance on the Public Contracts Regulations

	2015. In the event of a conflict between any current UK Government Guidance and the Crown Commercial Service Guidance, current UK Government Guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative Test	ESI tool completed by contractors on their own behalf at the request of the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information Security Management System	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency Event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium.
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR Claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 Assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Services but excluding know-how already in the Supplier's or the Buyer's possession before the Start Date.
Law	Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European

	Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Contract to be used by a Buyer to order Services.
Ordered Services	Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR
Processor	Takes the meaning given in the GDPR.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by the Buyer a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the

	performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: 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.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third-party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security Management Plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service Data	Data that is owned or managed by the Buyer and used for the Services, including backup data.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the Services for purposes of or in connection with this Contract.
Spend Controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start Date	The start date of this Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the Services or any part thereof or facilities or goods and services necessary for the provision of the Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract (permitted under

	the Contract) and its servants or agents in connection with the provision of Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Contract.
Supplier Terms	The relevant Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7 - GDPR Information

Annex 1 - Schedule of Processing, Personal Data and Data Subjects

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

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

Description	Details
Subject matter of the processing	Civil Service Jobs recruitment
Duration of the processing	TBC
Nature and purposes of the processing	Nature and purpose for collecting personal data are; 1. Personal Contact data is used to communicate with candidates and employees during the recruitment process. 2. Screening/Selection data is used to decide on candidate suitability for jobs that are applied to or to identify jobs for which we think candidates may be more suitable. Screening may be manual or automatic or a combination of both. 3. Evaluation data is used to record assessment of candidate suitability for jobs that the candidate is being considered for including status within the recruitment process. 4. Candidate feedback & tracking data is used to improve the recruitment process for future candidates. Tracking data is also used for programmatic advertising and to personalise the recruitment journey through the display of pertinent content. 5. Special Requirements data is used to make accommodation adjustments in the recruitment process for any needs participants may have. 6. Users can select to receive daily job alert emails based on their requirements, users can self-serve and unsubscribe. 7. Candidate Contractual Information and Other Contractual Information is used to compile contractual documentation (e.g. job offer and contract) and to record the contract. Candidate data may also be transferred to other systems that are under the control of the data controller, data processor and subcontractors (e.g. payroll systems, reporting tools). 8. On-Boarding Information is used to prepare for new hires starting work including setting up payroll information, benefits, and proof of right to work, including the transfer of information to other systems and subcontractors e.g. payroll systems, background checking agencies. 9. Equal Employment Opportunity Information is used to monitor the recruitment process to ensure recruitment practices are fair. 10. Data is used as part of aggregate data used by decision analytics, algorithms and reports to provide analysis, insights and predictions to help improve recruitment and drive efficiencies. 11. Data is erased as described under “Plan for return and destruction” 90 days after contract termination, at a subject’s request or by data retention schedule.In

	carrying out the above, the data is processed as follows: ● Collected via web forms and received by email from candidates, employees and subcontractors (such as recruitment agencies) ● Stored in a server farm ● Processed by computer including: performing calculations; evaluating information and recording results; reformatting information; analysing and the creation of algorithms, insights and predictions; ● Re-presented, transferred and communicated via web pages, email, and file transfers ● Erased and destroyed
Type of Personal Data	**Candidate account holders:** We will process the following personal data: When you create an account: ● Name ● Email address ● Your employer (civil servants only) ● Your line manager's email address (optional -for civil servants to verify their employment) Civil servants who are priority movers have the option to create a profile and add: ● Full contact details, including address ● Employer, role, grade and location ● Employment history ● Diversity and inclusion information When you view a job advert we may automatically collect: ● Your referral source - the website you saw the job advert ● Details of the pages you have viewed - including how long you spend on a page and which links you select ● Information about your computer - such as web browser used and device type ● Your approximate geographic location based on your IP address When you make an application we may ask for: ● Full contact details, including address ● Eligibility -nationality and immigration status ● Employment history ● Qualifications, licences and professional memberships ● Driving Licence ● diversity and inclusion information ● CV and personal statement ● Guaranteed Interview Scheme and reasonable adjustment requirements ● National Insurance number (Home Office vacancies only) When you are invited to an interview we may ask you to provide: ● Evidence of your identity and right to work in the UK -such as your passport, utility bills or other documentation When you undergo pre-employment checks we may ask for: ● Contact details for your referees ● National Insurance number ● Date of birth ● Public sector pension history ● Health declaration ● Driving licence ● Character declaration - including details of unspent convictions, motoring offences, police cautions, insolvency, bankruptcy, time spent outside of the UK and self-employment ● Addresses for the last 5 years ● Passport details ● previous names you were known by

	The list above only applies for applications made through the Civil Service Jobs system. Some advertisers may use their own application systems, when their privacy notice will apply. When you contact us with feedback or an enquiry we will process: ● Your email address ● The details of your request Individuals may not be asked for all this information at the same time. Successful candidates will be asked for more information than those who are rejected earlier in the recruitment process. **Staff (ATS) account holders:** ● Name ● Work email address ● Department **Beta Feedback**: ● User email captured ● Users may submit service improvement suggestions ● Volunteer for user testing ● Submit vacancy query to departments
Categories of Data Subject	● Users of the Civil Service Jobs website (www.civilservicejobs.service.gov.uk) who choose to create an account. When an account holder makes an application for a job, they will provide more data as part of their application. Not all account holders will make applications. ● Applicants –any adults (members of the public). ● Staff –those using the system to manage recruitment, manage the system, or use MI
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 personal data of applications will be kept for two years from the point that the vacancy is archived. This will be transferred back to the data controller, at their direction, at contract end. The data controller will also specify appropriate security controls to be in place during this transfer. The data processor will then delete the data, to a process as agreed with the data controller, within 90 days of contract termination.