Schedule 7B

Order Form for Competed Goods and Services- Mini Competition

[REDACTED]

The Authority	**Ministry of Justice**
The Supplier	**Softcat plc of Fieldhouse Lane, Marlow, Buckinghamshire, SL7 1LW (02174990)**
HealthTrust Europe Contract Reference	**MoJ VERIATO Remote User Security Monitoring Software** [REDACTED]

The Supplier and the Authority hereby agree as follows:

1. The Authority wishes to enter into a Contract in respect of the Services pursuant to the framework agreement between Health Trust Europe LLP and Supplier dated 2nd January 2024 (the "**Framework Agreement**").

2. The Contract incorporates, and the Supplier agrees to abide by, the following documents:
   (a) The Specification of the Authority's requirements as appended at Appendix 1 overleaf;
   (b) the Contract Price, as appended at Appendix 2 overleaf; and
   (c) the Call-Off Terms and Conditions set out at Appendix A to the Framework Agreement (including the front page and all Schedules thereto).

3. Where the Call-Off Terms and Conditions set out at **Error! Reference source not found.** of Appendix A to the Framework Agreement apply, the Authority acknowledges and agrees to the HealthTrust Europe Key Provisions, in particular as stated below for the avoidance of doubt:

   (a) The Authority acknowledges and agrees that the Supplier is subject to an activity based income (ABI) management charge in relation to any Orders placed by the Authority under the Framework Agreement.
   (b) The Authority and the Supplier agree that (in addition to the Authority's right to enforce the Contract) HealthTrust Europe may enforce any term of the Contract as principal in respect of ABI and Management Information and as agent on behalf of the Authority in respect of all other terms.

Annex 1 - Standard Terms

1 **Commencement Date and Term**

1.1 The Commencement Date of this Contract shall be **the date of the last signatures.**

1.2 The Term of this Contract shall be **3 years** from the Commencement Date and may be extended in accordance with Clause 15.2 of Schedule 2 of these Call-off Terms and Conditions provided that the duration of this Contract shall be no longer than 5 years in total. The initial term of the contract is three years, with the option to extend for an additional two years. The extension can be exercised in one-year increments, resulting in a possible contract duration of 3 + 1 + 1 years.

2 **Data Protection**

This Clause 2 only applies if this box is checked ☒

2.1 The Authority and the Supplier acknowledge and agree that it is their responsibility to carry out a data protection impact assessment ("**DPIA**") in accordance with the Data Protection Legislation and provided the DPIA confirms that the Supplier's systems and processes adequately provide the necessary guarantees to implement appropriate technical and organisational measures to comply with the Data Protection Legislation, they shall enter into the relevant data protection agreement.

2.2 The parties further acknowledge and agree that HealthTrust Europe will not be involved in or be responsible for the conduct of DPIAs and the supply of any data protection agreements (including a data protection protocol) required for Processing Personal Data under the Contract. For the avoidance of doubt, HealthTrust Europe accepts no responsibility in relation to any issues or claims related to the Processing of Personal Data by the Supplier for the Authority in pursuance of the Contract.

2.3 The Parties warrant that they have read, understood, and agree to the data protection provisions set out in Schedule 3 (Information and Data Provisions) of the Call Off Terms and Conditions.

2.4 The parties agree to comply with the Data Protection Protocol set out within Appendix 13.

3 **Payment Terms**

[REDACTED]

4 **Termination**

4.1 The Participating Authority may terminate this Contract forthwith by notice to the Supplier at any time on three (3) months' written notice. Such notice shall not be served within **3 years of the Commencement Date.**

5 **Locations**

The Services shall be provided, and Goods delivered by the Supplier at the Premises and Locations listed below:

5.1 Remotely

6 **Use of Subcontractors**

This Clause 6 only applies if this box is checked ☒

6.1 The Participating Authority grants permission for the Supplier to Sub-contract any of its obligations/ specific obligations under this Framework Agreement. This shall not impose any duty on the Participating Authority to enquire as to the competency of any authorised Sub-contractor. The Supplier shall ensure that any authorised Sub-contractor has the appropriate capability and capacity to perform the relevant obligations and that the obligations carried out by such Sub-contractor are fully in accordance with the Framework Agreement.

6.2 Where the Supplier sub-contracts the provision of any Goods and/or Services in pursuance of its contractual obligations under this Contract, the Supplier warrants and represents to the Participating Authority and to HealthTrust Europe that in addition to all other requirements related to subcontracting stated within the Framework Agreement, it shall remain the single point of contact and be responsible to HealthTrust Europe and the Participating Authority for all acts or omissions of the Sub-contractor or substitute Sub-contractor as though they were the Supplier's own acts or omissions for all elements of any Solution, including but not limited to Software and Equipment; and it shall ensure and shall procure that that its Sub-contractor(s) will deliver the Goods and/or Services in accordance with the terms of the Contract and in so doing, the Supplier shall:

6.2.1 strictly adherence to all KPI's and performance standards of the Contract and to all elements of the Specification;

6.2.2 immediately inform HealthTrust Europe and the Participating Authority in the event a Sub-Contractor fails, or becomes unable to meet any element of the Specification;

6.2.3 provide a list of all Sub-Contractors appointed at the Commencement Date as an annex to the Contract in the format set out below at Annex A of Appendix 11 (Subcontractors);

6.2.4 seek the prior written approval of the Participating Authority by following the Change Control Process if at any time during the Term the need arises to replace a Sub-Contractor listed in Annex A of Appendix 11 (Subcontractors), or to appoint a new Sub-Contractor.

6.3 The Supplier acknowledges and agrees that any proposed amendment to Annex A of Appendix 11 (Sub-contractors) shall be reserved as a right to the Participating Authority to: (i) consider any such amendment as a material variation of the Contract; (ii) reject the proposed change of Sub-Contractor; (iii) not accept Goods and/or Services from the any proposed new subcontractor; (iv) consider its option to re-tender for its requirements; and (v) without prejudice to any other rights reserved under the Contract terminate the Contract. The Participating Authority's approval shall not be unreasonably withheld or delayed.

6.4 The Supplier undertakes, warrants, and agrees that in order to meet its obligations under this Framework Agreement, it shall enter into contracts with its Sub-contractors that mirror the terms and conditions essential to perform the whole or the part(s) of its obligations which form the basis of the sub-contract. In any event, the Supplier shall ensure and shall procure that, as a minimum, its Sub-contractor will:

6.4.1 perform its obligations in accordance with the terms and conditions identical to those contained in the relevant contract with the Participating Authority;

6.4.2 acquire and maintain the same types and levels of insurance that will cover the risks required for performing under the relevant Contract;

6.4.3 where there will be Processing of Personal Data, the Supplier and the Sub-contractor will first conduct a data protection impact assessment (DPIA) on the operations of the Sub-contractor to ensure it has in place the appropriate security, technical and organisational measures to address the risks and ensure protection of personal data which demonstrate compliance with the data protection laws; and

6.4.4 cooperate fully in any audit or investigation undertaken by HealthTrust Europe or the Participating Authority in accordance with the call-off contract and the Framework Agreement.

6.5 In addition to all other rights reserved by HealthTrust Europe under the Framework Agreement, HealthTrust Europe hereby also reserves the right to conduct audits to: (i) ensure DPIAs are undertaken; (ii) review the due diligence process undertaken by the Supplier in relation to appointing Sub-contractors; and (iii) all other sub-contracting processes or changes thereto are compliantly undertaken. In this regard, the Supplier acknowledges and agrees that to ensure adherence to the terms and conditions of the Framework Agreement and any call-off contracts, it shall cooperate fully and procure that its Sub-contractor will cooperate fully in any such audits. Such audits will be conducted by HealthTrust Europe or its nominated agent(s), as and when deemed necessary, in the reasonable opinion of HealthTrust Europe, but in any event no more than once in a twelve (12) month period.

6.6 The bidding model that includes members of the supply chain, the percentage of work being delivered by each Sub-contractor and the key contract deliverables for which each Sub-contractor will be responsible are also detailed in Appendix 11 (Subcontractors).

7 **Contract Management**

The Contract Managers at the commencement of this Contract are:
[REDACTED]

8 **Notices**

Notices served under this Contract are to be delivered to:
[REDACTED]

9 In this Contract, unless the context otherwise requires, all capitalised words and expressions shall have the meanings ascribed to them by the Framework Agreement and/or Call-Off Terms and Conditions.

10 The following Annexes are incorporated within this Contract:

Annex 1	Standard Terms
Annex 2	Additional Key Provisions to Appendices 3 to 13 - Optional
Annex 3	Optional Terms for Software and related Services

11 The following Appendices are incorporated within this Contract:

Appendix 1	Participating Authority Specification
Appendix 2	Contract Price
Appendix 3	Change Control Process
Appendix 4	Implementation Plan
Appendix 5	Locations subject to lease and/or licence
Appendix 6	Step In Rights
Appendix 7	Termination Sum
Appendix 8	TUPE Transfer
Appendix 9	Software and End User License Agreement (EULA)
Appendix 10	Key Performance Indicators
Appendix 11	Subcontractors
Appendix 12	Social Value
Appendix 13	Data Protection Protocol Form

Signed by the authorised representative of THE PARTICIPATING AUTHORITY

Name:	[REDACTED]	Signature:	[REDACTED]
Position:	[REDACTED]	Date:	[REDACTED]

AND

Signed by the authorised representative of THE SUPPLIER

Name:	[REDACTED]	Signature:	[REDACTED]
Position:	[REDACTED]	Date:	[REDACTED]

Appendix 1
Authority Specification

Must have functional requirements

REF	Functional Requirement
	The remote monitoring solution will have the following capabilities
FR0010	· Capture all keystrokes for all user types
FR0020	· Monitoring and alerting to MoJ's XSIAM on key words typed by a user on a desktop
FR0030	· Monitoring and alerting to MoJ's XSIAM on key phrases typed by a user on a desktop
FR0060	· Ability to maintain key words lists, including adding and removing key words from the lists
FR0070	· Ability to maintain key phrases lists, including adding and removing key phrases from the lists
FR0080	· Ability to maintain number sequences lists, including adding and removing from the lists
FR0100	· Periodic screen capture. The time between screen capture must be configurable (e.g. every eight seconds)
FR0110	· Ability to review activity logs by user, time, or location
FR0120	· All captured data and alerts to be stored for a configurable time period (currently set to 90 days)
FR0130	· Ability to archive select logged data for a configurable time period
FR0140	The remote monitoring solution shall automatically launch when an authorised user logs into a desktop or laptop that hosts the remote monitoring solution
FR0150	The remote monitoring solution shall be able to detect and alert on a user account that is simultaneously logged into two or more desktops or laptops within a single or multiple establishments
FR0160	The solution shall have role-based access control (RBAC) to cater for different user types and privileges

Should have functional requirements

REF	Functional Requirement
	The remote monitoring solution will have the following capabilities
FR0040	· Monitoring and alerting to MoJ's XSIAM on key number sequences typed by a user on a desktop
FR0050	· Monitoring and alerting to MoJ's XSIAM on websites that have been marked for alerting where the user has attempted to access that website
FR0080	· Ability to maintain website alert lists, including adding and removing website URLs from the lists

Non-Functional Requirements

REF	Non-Functional area	Summary	Non-Functional Requirement
NFR0010	Accessibility	Accessibility capability	The solution shall meet current accessibility standards WCAG 2.2: https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag
NFR0020	Data management	Data centre security standards	The supplier's Data Centre security standards shall comply with the CSA CCM version 3.0 standard
NFR0030	Data management	Data classification	The supplier shall treat all data as 'Official Sensitive'
NFR0040	Data management	Data ownership	The supplier acknowledges that the contracting authority shall be the data owner and the supplier shall be the data processor
NFR0050	Data management	Data rectification	The supplier shall be able to rectify incorrect data with associated audit trail recording and under guidance with the contracting authority
NFR0060	Data management	GDPR compliance	The solution shall meet the MoJ's GDPR policy requirements
NFR0090	Data management	Personal data anonymisation for testing	The solution shall not use live personal data for the purposes of testing or training
NFR0110	Data management	UK hosted data	Supplier-based hosting of MoJ data shall reside in the UK and be protected in line with current data regulations applicable under UK law.
			Exceptionally, and in agreement with the contracting authority, the supplier shall be able to host MoJ data in a country, which is part of the EEA.

			Where MoJ data is hosted in an EEA country, the supplier and contracting authority shall agree a plan to migrate the MoJ data to the UK.
NFR0120	Government standards	Compliance with Government and MoJ Security standards	
			The supplier shall comply to or be capable of complying with the following standards:
			• MoJ IT Security Standards
			• Demonstrable plan for achieving Cyber Essentials Plus for contract start
			• ISO27001/2 Certification
			· The principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework
			· The Government Security - Classification policy: https://www.gov.uk/government/publications/government-security-classifications
			• Guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.npsa.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.npsa.gov.uk/sensitive-information-assets
			· The National Cyber Security Centre's (NCSC) information risk management guidance: 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: The Technology Code of Practice - GOV.UK (www.gov.uk)
			· The security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
NFR0130	Security	APIs	Where supplier access to Authority Systems uses or depends upon API credentials (such as providing a token or other credential for use during authentication, authorisations, or access control to an API endpoint), the supplier shall use industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed and during storage.
NFR0140	Security	Audit capability	The solution shall be able to collect and provide auditable logs on system usage, and shall be accessible to the contracting authority
NFR0150	Security	Connectivity and cryptographic standards	The supplier shall ensure technical solutions and services adopt and fully comply with modern connectivity and cryptographic standards after applicable guidance and standards have been updated, including but not limited to, implementing iterations to in-transit encryption such as Transport Layer Security (TLS) minimum 1.2, and Internet Protocol Security (IPSec) and at-rest encryption.

NFR0160	Security	Continuous review of technical security measures	The supplier shall continuously review technical security measures to ensure any appropriate, applicable and proportional changes are applied in response to, and in accordance with, changes to government and industry guidance.
NFR0170	Security	IT Health Checks (ITHCs)	The solution shall be subject to ITHCs, using a CHECK accredited organisation:
			• Upon commissioning the service
			• Yearly thereafter (or other frequency agreed with the contracting authority)
			• As a result of major changes to the solution
NFR0190	Security	Security Management Plan	The supplier shall produce a Security Management Plan, within 20 working days of the start date, which will include (but is not limited to) the following:
			• Approach to ITHCs
			• Approach to ongoing compliance with MoJ security policy
			• A description of threat and vulnerability tools that will be used to help secure the application
			• Incident management response
NFR0200	Security	Security risk assessments	The Supplier shall undertake risk assessment(s) of any component, including but not limited to systems, services, personnel, physical locations and supply chain (including all Sub-contractors and Sub-Processors), utilised or otherwise involved in the provision of the Services
NFR0210	Security	Supplier staff clearance	The supplier shall ensure clearance levels for staff are:

			• Access to live MoJ systems and / or MoJ data: SC level and resides in the UK
			• No access to live systems and / or MoJ data: BPSS level
NFR0220	Security	Supplier's staff security training	Supplier personnel shall be provided with adequate and relevant security-related education, training and awareness and include, but not be limited to, technical, physical and procedural security.
			This shall be completed annually with proof of certification provided to the authority.
NFR0230	Service Management	Business Continuity and Disaster Recovery testing	The solution shall be tested, at least annually, in accordance with the Supplier's Business Continuity and Disaster Recovery plans
NFR0240	Service Management	Business Continuity plan	The solution shall be supported by a Business Continuity plan, which must be agreed with the contracting authority
NFR0250	Service Management	Compliance with ITIL standard	The supplier and solution shall be able to comply or be capable of complying with ITIL standards
NFR0260	Service Management	Disaster Recovery plan	The solution shall be supported by a Disaster Recovery plan, which must be agreed with the contracting authority, the plan shall include:
			• Recovery Point Object (RPO)
			• Recovery Time Object (RTO)
NFR0270	Service Management	Failover	Please describe your failover capabilities.

NFR0280	Service Management	Proactive monitoring	The supplier shall have in place proactive monitoring of the solution, including:
			• operation of the solution
			• security of the solution including anti-virus, malware scans and protection (such as denial of service mitigation), vulnerability scanning and management, intrusion and data loss prevention
			• availability of the solution including incident response, and incident escalation and investigation
NFR0290	Service Management	Service management - SLAs	As part of your response please tell us your SLAs for:
			[REDACTED]
			Root cause analysis turnaround • Upon request, for Priority 1 incidents. • Within 72 hours of delivered and verified working resolution.
NFR0300	Service Management	Incident response	The supplier shall work within the following target incident resolution timescales:
			Priority 1:
			• Significant disruption to critical business activities; many users affected across many sites; major impact on business
			• Target response - 10 minutes
			• Target resolution – Four hours following root cause determination
			Priority 2:

			• Some disruption to business activities; subset of users affected
			• Target response - 30 minutes
			• Target resolution – Eight hours following root cause determination
			Priority 3:
			• More than one user affected: moderate business impact
			• Target response – One hour
			• Target resolution – Two days following root cause determination
			Priority 4:
			• Single user affected
			• Target response – Four hours
			• Target resolution – Five days following root cause determination
NFR0310	Service Management	Service Management reviews	The supplier shall attend regular service performance review meetings to discuss service performance and service improvement activities.
NFR0320	Service Management	Service Management reviews - reporting	The supplier shall make available service performance reports and key statistics (to be agreed with the contracting authority) in relation to the solution; in a frequency and format as determined by the contracting authority. Please provide a sample of such performance reports and key statistics as part of your response.
NFR0330	Service Management	Service Manager support	The supplier shall make available a service manager who will be available:
			• during working hours (9am to 5pm (GMT) - Monday to Friday - excluding bank holidays)

			• duration of the contracted services
NFR0340	Service Management	Out of hours service support	The Supplier shall provide a facility to allow the Buyer to log tickets online out of hours.
NFR0350	Service Management	Service support hours	The supplier shall provide helpdesk support 8am to 6pm (UK time), Monday to Frid
NFR0360	System	Browser compatibility	The solution shall be able to run on multiple browser versions including Edge and Chrome
			https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices
NFR0370	System	Cloud based	The solution shall be a cloud based solution - Software as a Service
NFR0380	System	Integration with AAD	The solution shall be capable of integration with Azure Active Directory (AAD) and any synchronisation shall be immediate.
NFR0400	System	Windows version	The solution shall be compatible with the current and previous versions of the Windows Operating system
NFR0410	Solution performance, scalability, and availability	Solution availability	The solution shall have an up time of 99.5% during operational hours. Operational hours are defined as follows:
			• Monday to Friday – 6am to 8pm (GMT)
			• Saturday and Sunday – 8am to 4pm (GMT)
NFR0420	Downtime	Downtime for maintenance	The solution supplier shall ensure that downtime for systems maintenance shall fall outside the following hours:
			• Monday to Friday – 6am to 8pm (GMT)
			• Saturday and Sunday – 8am to 4pm (GMT)

NFR0430	Volumetrics	Number of concurrent desktops / users	The remote monitoring solution shall be scalable up to 9,000 devices in concurrent use
NFR0440	Operational working agreement	Operational working agreement	The Supplier of the remote monitoring solution and the Buyer shall produce an Operational Working Agreement to identify, document and agree the day-to-day operational processes and obligations between the Supplier and the Buyer
NFR0450	Planned maintenance	Planned maintenance	The Supplier shall give the Buyer at least seven days' notice of any planned maintenance and downtime of the solution.
NFR0460	Product MI & Reporting	Product MI & Reporting	The Supplier shall make available: • Buyer access to the built in standard MI & reporting suite, which is part of the Veriato System • Buyer to be able to request ad-hoc, bespoke management information requests

Should have non-functional requirements

REF	Non-Functional area	Summary	Non-Functional Requirement
NFR0070	Data management	Interface to export data	The solution shall be able to provide an interface to export reporting data to the authority's reporting platform.

Appendix 2
Contract Price

[REDACTED]

1. Purpose

Subject to Clause 17 (Benchmarking and Value for Money) of the Framework Agreement, this Appendix 2 outlines the terms relating to agreement of the Contract Price (as detailed in Part 1) between the Participating Authorities and the Supplier applicable to Years 2 to 5 of the Term. The Parties agree that the Contract Price may fluctuate due to currency fluctuations and other relevant economic factors.

2. Definitions
For the purposes of this Appendix, the following terms shall have the meanings set out below:

a) Term: The duration of the Call off Contract, which is five (5) years.

b) Fixed Pricing Period: The initial year (year 1) of the Term, during which prices are fixed and not subject to change.

c) Currency Fluctuation: Years 2 & 3 of the Term, during which prices may be subject to change due to currency fluctuation.
Changes in the exchange rate between the currency in which the Contract Price is priced and the Supplier's operational currency.
The Fees to be paid by the Customer for years 2 and 3 shall be calculated on the relevant anniversary dates based on the currency exchange rates applicable on those days. All costs related to providing the license must be included in the agreed price.

c) Price change: Years 4 & 5 not fixed and subject to pricing increases.

d) Pricing Review Date: The date set as 60 days prior to the start date of year 2 (and then annually thereafter) at which the Contract Price for the forthcoming year will be reviewed.

g) Proposed Contract Price: the pricing submitted in writing by the Supplier by the Pricing Review Date subject to the Buyers approval in accordance with section 5 below.

3. Fixed Pricing Period

3.1 The Contract Price for all goods and services provided under the Call off Contract during the Fixed Pricing Period shall be fixed and not subject to any increases or adjustments.

4. Variable Pricing Period

4.1 The Contract Price for goods and services provided under the Call off Contract during the Variable Pricing Period may be adjusted annually in accordance with the terms set out in this Appendix 2.
4.2 Prior to each Pricing Review Date, the Supplier shall review and submit the Proposed Contract Price for the forthcoming year and may propose adjustments (any increases in respect of years 2 and 3 to be capped at 10% per year) based on the following factors:

a) Currency Fluctuations: Adjustments due to changes in the exchange rate between the currency in which the Call off Contract is priced and the Supplier's operational currency. Unless otherwise agreed in writing between the Parties, for the purposes of this Call-off Contract, a transaction rate of 1.28 (3 points below the market live rate) shall be the baseline for any currency fluctuation adjustments in years 2 and 3.
b) Economic Factors: Other relevant economic factors that may impact the cost of providing the goods and services, such as inflation, changes in supplier costs, or changes in regulatory requirements.

4.3 The Supplier must provide (with the Proposed Contract Price) a detailed explanation of the reasons for the proposed adjustments, including the specific factors contributing to the price change including documentation supporting the proposed adjustments, such as exchange rate data or inflation indices.

5. Extension Period

5.1 Notwithstanding any other payment terms or pricing contained herein, the Parties agree that should the Customer wish to make use of the optional extension periods at the end of the initial term, then the Supplier shall have a right to adjust the commercial pricing to accurately reflect any fluctuation or movement in exchange rates, in addition to any other agreed pricing increases. Each party shall cooperate with the other and act in good faith to take further steps as appropriate to implement these reasonable pricing changes.

5.2 The extension and any associated charges are subject to agreement in writing between the Customer and the Supplier. The Supplier shall, when converting US Dollars to GBP sterling at the then current applicable rate, issue appropriate amended invoices, and any other documents necessary for that purpose.

6. Review and Approval

6.1 The Participating Authorities shall have sixty (60) days from receipt of the Proposed Contract Price to review the proposed adjustments.

6.2 The Participating Authorities may:
(a) accept the proposed adjustments and the Proposed Contract Price shall become the Contract Price; or
(b) request further documentation or clarification; or
(c) negotiate the proposed adjustments with the Supplier.

6.3 Subject to Schedule 10 (Change Control Process) all changes shall be documented in writing and signed by both parties.

7. Dispute Resolution

7.1 Any disputes shall be resolved in accordance with the Dispute Resolution Procedures set out in Clause 22 of Schedule

8. Out-of-Scope Work and Rate Card

Any services or work requested by the Client that fall outside the scope of the agreed deliverables outlined in this contract shall be subject to the rates set forth in the attached Rate Card. Such out-of-scope work will only be undertaken upon written approval from the Client.

The parties agree that the Rate Card outlines the applicable hourly/daily rates for additional work, and (subject to clause 4 above) these rates shall apply to all approved out-of-scope tasks. Clause 4 of Appendix 2 above (variable pricing period) shall also apply in respect of the Rate Card pricing.

[REDACTED]

Appendix 3
Change Control Process

[REDACTED]

Appendix 4
Implementation Plan

The parties agree to finalise the implementation plan within 14 working days of signing the contract.

Appendix 5
Lease and/or Licence to access Premises and Locations

Not Applicable

Appendix 6
Step In Rights

Not Applicable

Appendix 7
Termination Sum

Not applicable with minimum commitment of 3 years

Appendix 8
Staff Transfer

Not Applicable

Appendix 9

Software and End-User Licence Agreement (EULA)

As included below:

[REDACTED]

Appendix 10

Key Performance Indicators (KPIs)

These Key Performance Indicators are intended as templates for each Participating Authority, they may be amended as applicable to each subsequent contract, subject to the Participating Authority's requirements.

(A) *The KPIs which the Parties have agreed shall be used to measure the performance of the Services by the Supplier are contained in the below table.*
(B) *The Supplier is required to manage and provide the Services in such a way as to meet the KPIs.*
(C) *The Supplier shall monitor its performance against each Target KPI and shall send the Participating Authority a quarterly report detailing the achieved KPIs in a form and format to be mutually agreed.*

The KPIs relating to this Contract are as follows: -
[REDACTED]

1 *Monitoring Performance*
[REDACTED]

2 *Service Level Failure*

2.1 *A Service Level Failure shall occur where, in any one-month period:*

Red Event	*Registered against two KPIs*
Black Event	*Registered against one KPI*

Service Credits

2.2 *If there is a Service Level Failure, the Supplier shall:*
2.2.1 *notify the Participating Authority immediately of the Service Level Failure;*
2.2.2 *provide the Participating Authority with a draft remediation plan which sets out the steps to be taken by the Supplier in order to remedy the Service Level Failure and prevent recurrence ("**Remediation Plan**");*
2.2.3 *deploy all additional resources and take all remedial action that is necessary to rectify or to prevent the Service Level Failure from recurring; and*
2.2.4 *carry out the actions identified in Remediation Plan in accordance with its terms.*

2.3 *Other than in the following circumstances:*
2.3.1 *Any negligent act or omission of the Participating Authority;*
2.3.2 *Any breach of an express provision of this Contract by the Participating Authority;*
2.3.3 *Any Force Majeure Event;*

If there is a Service Level Failure, the Participating Authority shall be entitled to a Service Credit equal to 2% of the price payable for support (listed in Appendix 2), payable for affected service element(s) in that pro-rated Month period.

Service Credits shall, at the election of Service Provider, either (i) be shown as a deduction from the amount due from the Participating Authority to the Supplier in the next invoice then due to be issued under this Contract, (ii) satisfied by Supplier issuing a credit note against a previous invoice and the amount for the Service Credits shall be repayable by the Supplier as a debt within thirty (30) Business Days of issue of the termination of this Contract, or (iii) satisfied by the provision of additional days of service under this Contract, such additional days calculated pro-rata based on

the Contract amount and the total number of days of the Contract term. The parties agree that any such Service Credits have been calculated as, and are, a genuine pre-estimate of the loss likely to be suffered by the Participating Authority.

The aggregate Service Credits for any month shall be capped at [three (3) Service Credits or 6% of the price payable for support (listed in Appendix 2) for that pro-rated month]
Relief Event means
(i) any breach of any express provision of this Contract by the Participating Authority including without limitation an obligation to comply with the Participating Authority's obligations;
(ii) any negligent act or omission of the Participating Authority;
any Force Majeure Event

Appendix 11
Sub-Contractors

Annex A
List of Sub-Contractors

In exercise of its right under Clause 28.1 of Schedule 2 (General Terms and Conditions of these Call-off Contract), the Participating Authority hereby authorises the appointment by the Supplier of the following Sub-Contractors for the purpose of this Contract:

[REDACTED]

Appendix 12
Social Value

MoJ Requirement

Social Value
1. Tackling economic inequality Policy Outcome: Increase supply chain resilience and capacity Award Criteria: Demonstrate collaboration throughout the supply chain, and a fair and responsible approach to working with supply chain partners in delivery of the contract.

Softcat has proposed commitments which it will aim to achieve over the agreement length and has proposed the following structure as part of its method statement.

1. After on-boarding, Softcat and MoJ to work together to define a Social Value plan. This may follow the format seen in the 'MAC 2.2. – Timed Action Plan' document below.
2. Softcat will use the Social Value Plan as a framework to achieve its commitments.
3. Softcat will provide reporting against achievement as an agenda item against Quarterly Business Reviews, and will provide annually released reporting to further support.

Timed Action Plan – Template

[REDACTED]

Softcat Method Statement

[REDACTED]

Appendix 13A

DATA PROTECTION PROTOCOL

The Parties acknowledge that there is no intention for the Supplier to process any Customer Personal Data under this contract for the purpose of providing the deliverables, other than that which is detailed in the MoJ Security Management: Authority Led Assurance Protocol. Any Personal Data Processing necessary for providing the deliverables under this contract is to be done by the Supplier's Subcontractor, Veriato, in accordance with the Veriato DPA below.

[REDACTED]

Guidance: This Security Management: Authority-Led Assurance Protocol is for use alongside the NHS terms and conditions.

SECURITY MANAGEMENT: AUTHORITY LED ASSURANCE

[REDACTED]

APPENDIX 13B

DYNAMIC FRAMEWORK
PROCESSING PERSONAL DATA

MoJ Data Protection schedule which has been approved by Information Security Team.

[REDACTED]

Definitions

The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract shall also apply to this Protocol. For example, the following terms are defined in Schedule 4 of the Contract: "Authority", "Data Protection Legislation", "UK GDPR", "Process" and "Processor" and "Supplier" are defined in Schedule 4 of the Contract. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

"Controller"	shall have the same meaning as set out in the UK GDPR;
"**Data Protection Impact Assessment**"	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"**Data Protection Officer**"	shall have the same meaning as set out in the UK GDPR;
"**Data Recipient**"	means that Controller who receives the relevant Personal Data;
"**Data Subject**"	shall have the same meaning as set out in the UK GDPR;
"**Data Subject Request**"	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"**Data Transferor**"	means that Controller who transfers the relevant Personal Data;
"**Information Commissioner**"	means the Information Commissioner in the UK;
"**Joint Controllers**"	means where two or more Controllers jointly determine the purposes and means of Processing;
"**Personal Data Breach**"	shall have the same meaning as set out in the UK GDPR;
"Processor"	shall have the same meaning as set out in the UK GDPR;

"**Protocol**" or "**Data Protection Protocol**"	means this Data Protection Protocol;
"**Sensitive Data**"	shall mean the types of data set out in Article 9(1) or 10 of the UK GDPR;
"**Sub-processor**"	means any third Party appointed to Process Personal Data on behalf of that Processor related to this Contract.

1. Supplier as data processor

1.1 Purpose and scope

1.1.1 The purpose of this Clause 1 is to ensure compliance with Article 28(3) and (4) of the UK GDPR.

1.1.2 This Clause 1 applies to the Processing of Personal Data as specified in Table A.

1.1.3 Table A is an integral part of this Clause 1.

1.1.4 This Clause 1 is without prejudice to obligations to which the Controller is subject by virtue of the UK GDPR.

1.1.5 This Clause 1 does not by itself ensure compliance with obligations related to international transfers in accordance with Chapter V of the UK GDPR.

1.2 Invariability of Clause 1

1.2.1 The Parties undertake not to modify Clause 1, except for adding information to Table A or updating information in it.

1.2.2 This does not prevent the Parties from including the standard contractual clauses laid down in this Clause 1 in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict Clause 1 or detract from the fundamental rights or freedoms of Data Subjects.

1.3 Interpretation

1.3.1 Where this Clause 1 uses the terms defined in the UK GDPR, those terms shall have the same meaning as in the UK GDPR.

1.3.2 This Clause 1 shall be read and interpreted in the light of the provisions of the UK GDPR.

1.3.3 This Clause 1 shall not be interpreted in a way that runs counter to the rights and obligations provided for in the UK GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

1.4 Hierarchy

1.4.1 In the event of a contradiction between this Clause 1 and the provisions of the Contract and/or related agreements between the Parties existing at the time when this Clause 1 is agreed or entered into thereafter, this Clause 1 shall prevail.

1.5 Description of the processing

1.5.1 The details of the Processing operations, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of the Controller, are specified in Table A.

1.6 Obligations of the Parties

1.6.1 Instructions

(i) The Processor shall Process Personal Data only on documented instructions from the Controller, unless required to do so by Law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before Processing, unless the Law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the Processing of Personal Data. These instructions shall always be documented.

(ii) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the UK GDPR.

1.6.2 Purpose Limitation

(i) The Processor shall Process the Personal Data only for the specific purpose(s) of the Processing, as set out in Table A, unless it receives further instructions from the Controller.

1.6.3 Duration of the Processing of Personal Data

(i) Processing by the Processor shall only take place for the duration specified in Table A.

1.6.4 Security of Processing

(i) The Processor shall at least implement the technical and organisational measures specified in Table A to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

(ii) The Processor shall grant access to the Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Contract. The Processor shall ensure that persons authorised to Process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.6.5 Sensitive Data

(i) If the Processing involves Sensitive Data as set out in Table A, or data relating to criminal convictions and offences, the Processor shall apply specific restrictions and/or additional safeguards as agreed between the Parties in Table A.

1.6.6 Documentation and compliance

(i) The Parties shall be able to demonstrate compliance with this Clause 1.

(ii) The Processor shall deal promptly and adequately with inquiries from the Controller about the Processing of data in accordance with this Clause 1.

(iii) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in this Clause 1 and stem directly from the UK GDPR. At the Controller's request, the Processor shall also permit and contribute to audits of the Processing activities covered by this Clause 1, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

(iv) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice.

(v) The Parties shall make the information referred to in this Clause 1, including the results of any audits, available to the Information Commissioner on request.

1.6.7 Use of Sub-processors

(i) The Processor shall not subcontract any of its Processing operations performed on behalf of the Controller in accordance with this Clause 1 to a Sub-processor, without the Controller's prior specific written authorisation. The Processor shall submit the request for specific authorisation at least fourteen (14) days prior to the engagement of the Sub-processor in question, together with the information necessary to enable the Controller to decide on the authorisation.

(ii) Where the Processor engages a Sub-processor for carrying out specific Processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the Sub-processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with this Clause 1. The Processor shall ensure that the Sub-processor complies with the obligations to which the Processor is subject pursuant to this Clause 1 and to the UK GDPR.

(iii) At the Controller's request, the Processor shall provide a copy of such a Sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Processor may redact the text of the agreement prior to sharing the copy.

(iv) The Processor shall remain fully responsible to the Controller for the performance of the Sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-processor to fulfil its contractual obligations.

(v) The Processor shall agree a third party Customer clause with the Subprocessor whereby - in the event the Processor has factually disappeared, ceased to exist in law or has become insolvent - the Controller shall have the right to terminate the Sub-processor contract and to instruct the Sub-processor to erase or return the Personal Data.

1.6.8 International Transfers

(i) Any transfer of data to a third country or an international organisation by the Processor shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Law to which the Processor is subject and shall take place on the basis of an adequacy regulation (in accordance with Article 45 of the UK GDPR) or standard data protection clauses (in accordance with Article 46 of the UK GDPR). All transfers shall comply with Chapter V of the UK GDPR and any other applicable Data Protection Legislation.

(ii) The Controller agrees that where the Processor engages a Sub-processor in accordance with Clause 1.6.7. for carrying out specific Processing activities (on behalf of the Controller) and those Processing activities involve a transfer of Personal Data within the meaning of Chapter V of GDPR, the Processor and the Sub-processor can ensure compliance with Chapter V of the UK GDPR by using standard contractual clauses adopted by the Information Commissioner in accordance with Article 46(2) of the UK GDPR, provided the conditions for the use of those standard contractual clauses are met.

1.7 Assistance to the Controller

1.7.1 The Processor shall promptly notify the Controller if it receives a Data Subject Request. It shall not respond to the request itself, unless authorised to do so by the Controller.

1.7.2 The Processor shall assist the Controller in fulfilling its obligations to respond to Data Subject Requests to exercise their rights, taking into account the nature of the Processing. In fulfilling its obligations in accordance with Clauses 1.7.1 and 1.7.2 Processor shall comply with the Controller's instructions.

1.7.3 In addition to the Processor's obligation to assist the Controller pursuant to Clause 1.7.2, the Processor shall furthermore assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data Processing and the information available to the Processor:

(i) the obligation to carry out a Data Protection Impact Assessment where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

(ii) the obligation to consult the Information Commissioner prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(iii) the obligation to ensure that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated; and

(iv) the obligations in Article 32 of the UK GDPR.

1.7.4 The Parties shall set out in Table A the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause 1.7 as well as the scope and the extent of the assistance required.

1.8 Notification of Personal Data Breach

1.8.1 In the event of a Personal Data Breach, the Processor shall co-operate with and assist the Controller to comply with its obligations under Articles 33 and

34 of the UK GDPR, where applicable, taking into account the nature of Processing and the information available to the Processor.

1.8.2 Personal Data Breach concerning data Processed by the Controller

(i) In the event of a Personal Data Breach concerning data Processed by the Controller, the Processor shall assist the Controller:

(A) in notifying the Personal Data Breach to the Information Commissioner, without undue delay after the Controller has become aware of it, where relevant (unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(B) in obtaining the following information which, pursuant to Article 33(3) of the UK GDPR, shall be stated in the Controller's notification, and must at least include:

1) the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

2) the likely consequences of the Personal Data Breach; and

3) the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(C) in complying, pursuant to Article 34 of the UK GDPR, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

1.8.3 Personal Data Breach concerning data Processed by the Processor

(i) In the event of a Personal Data Breach concerning data Processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

(A) a description of the nature of the breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);

(B) the details of a contact point where more information concerning the Personal Data Breach can be obtained; and

(C) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(ii) The Parties shall set out in Table A all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under Articles 33 and 34 of the UK GDPR.

1.9 ***Non-compliance with Clause 1 and termination***

1.9.1 Without prejudice to any provisions of the UK GDPR, in the event that the Processor is in breach of its obligations under this Clause 1, the Controller may instruct the Processor to suspend the Processing of Personal Data until the latter complies with this Clause 1 or the Contract is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this Clause 1 for whatever reason.

1.9.2. The Controller shall be entitled to terminate the Contract insofar as it concerns Processing of Personal Data in accordance with this Clause 1 if:

(i) the Processing of Personal Data by the Processor has been suspended by the Controller pursuant to Clause 1.9.1 and if compliance with this Clause 1 is not restored within a reasonable time and in any event within one month following suspension;

(ii) the Processor is in substantial or persistent breach of this Clause 1 or its obligations under the UK GDPR;

(iii) the Processor fails to comply with a binding decision of a competent court or the Information Commissioner regarding its obligations pursuant to this Clause 1 or to the UK GDPR.

1.9.3 The Processor shall be entitled to terminate the Contract insofar as it concerns Processing of Personal Data under this Clause 1 where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 1.6.1(ii), the Controller insists on compliance with the instructions (provided that the Processor has clearly demonstrated the infringement by the provision of a legal opinion provided by a solicitor or barrister that both Parties can rely upon).

1.9.4 Following termination of the Contract, the Processor shall, at the choice of the Controller, delete all Personal Data Processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the Personal Data to the Controller and delete existing copies unless the Law requires storage of the Personal Data. Until the data is deleted or returned, the Processor shall continue to ensure compliance with this Clause 1.

2. Parties as joint controllers

2.1. Where in Table A the Parties acknowledge that, for the purposes of the Data Protection Legislation, the Authority and the Supplier are Joint Controllers, this Clause 2 shall apply. The only Processing that a Joint Controller is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.

2.2. The Parties shall, in accordance with Article 26 of the UK GDPR, enter into a Joint Controller agreement based on the terms outlined in Annex 1.

3. Both data controllers

3.1. To the extent that the nature of the Supplier's obligations under the Contract means that the Parties are acting both as Controllers (as may be referred to in Table A), each Party undertakes to comply at all times with its obligations under the Data Protection Legislation and shall:

3.1.1. implement such measures and perform its obligations (as applicable) in compliance with the Data Protection Legislation; and

3.1.2. be responsible for determining its data security obligations taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, and shall implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful Processing and accidental destruction or loss and ensure the protection of the rights of the Data Subject, in such a manner that Processing will meet the requirements of the Data Protection Legislation where Personal Data has been transmitted by it, or while the Personal Data is in its possession or control.

3.2. Where Personal Data is shared between the Parties, each acting as Controller:

3.2.1. the Data Transferor warrants and undertakes to the Data Recipient that such Personal Data has been collected, Processed and transferred in accordance with the Data Protection Legislation and this Clause 1;

3.2.2. the Data Recipient will Process the Personal Data in accordance with the Data Protection Legislation and this Clause 1; and

3.2.3. where the Data Recipient is in breach of its obligations under this Protocol and the Data Protection Legislation, the Data Transferor may suspend the transfer of the Personal Data to the Data Recipient either on a temporary or permanent basis, depending on the nature of the breach.

Guidance: there are limited requirements in the UK GDPR when Parties act as separate Controllers. Clause 3 above provides a sensible starting point. However, Authorities are advised to review the Information Commissioner's guidance (ICO GDPR Guidance) and consultant their Information Governance team when considering whether further provisions or a separate data sharing agreement should be used

4. Changes to this protocol

4.1 Any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

Annex 2 - Optional Terms for Key Provisions

Call off Contract ☒ (only applicable to the Contract if the box is checked and the standards or requirements are listed)

1 Provision of Goods and Services - Delivery Standards ☒

1.1 **In-house Services by Supplier** - Time is of the essence as to any delivery dates under this Contract. If the Supplier fails to meet any delivery date this shall be deemed to be a breach incapable of remedy for the purposes of Clause 15.4.(i) of Schedule 2 of these Call-off Terms and Conditions.

1.2 **Goods and Services by Sub-contractors, manufacturers or third parties** – The Supplier shall use reasonable endeavours to meet any performance dates specified in the Order Form or in this Contract. If the Supplier fails to do so, the Participating Authority may without prejudice to any other rights it may have under the Contract:

(a) terminate the Order in whole or in part without liability to the Supplier;
(b) refuse to accept any subsequent delivery of the Goods or performance of the Services (as the case may be);
(c) purchase substitute Goods and/or Services from another supplier; and
(d) hold the Supplier accountable for any losses and additional costs incurred.

2 Provision of Goods – Inspection of Goods ☐

2.1 For the purposes of Clause [insert] of [insert Schedule], the Participating Authority shall visually inspect the Goods within [insert **time period** during which any inspection must be carried out] of the date of delivery of the relevant Goods.

3 Provision of Services - (Long Stop Date(s))* ☐

[*only use if the Services are to start at a different date following the Commencement Date].

3.1 The Services Commencement Date shall be **[insert date]**

3.2 The Long Stop Date for the commencement of provision of the Services shall be **[insert date].**

4 Training, Support Services and/or Help Desk ☐

4.1 The Supplier or its Sub-contractor shall as soon as reasonably practicable after delivery of the Goods or Services to the Participating Authority, provide a suitably qualified professional to deliver a thorough training programme about the features and benefits of the Goods and Services the Participating Authority.

4.2 The Supplier shall provide as much training and support to the Participating Authority as the Participating Authority may reasonably require throughout the Term. Such training shall be carried out within the Contract Price and any associated costs shall be absorbed in full by the Supplier.

4.3 The Supplier shall at its own expense provide the Participating Authority with copies of all training materials and resources, such materials to include a [insert]with sufficient detail to enable trained [clinical or applicable] staff within the Participating Authority to train others.

5 Implementation and Acceptance Testing of Goods and Services – Implementation Plan ☐

5.1 The Supplier shall implement the Services in accordance with the Implementation Plan appended at Appendix 4.

6 Implementation and Acceptance Testing of Goods and Services – Pre-Acceptance Criteria ☐

6.1 The parties agree to adhere to the Pre-Acceptance Criteria detailed within [insert]

7 Implementation and Acceptance Testing of Goods and Services – Provisional Acceptance Criteria ☐

7.1 The parties agree to adhere to the Provisional Acceptance Criteria detailed within [insert]

8 Implementation and Acceptance Testing of Goods and Services – Final Acceptance Criteria ☐

8.1 The parties agree to adhere to the Final Acceptance Criteria detailed within [insert].

8.2 Once the Supplier has completed all elements of delivery and installation/ implementation of the Goods and/or Services and has notified the Participating Authority in writing of such, the Participating Authority shall have, as a minimum, **[insert]** Business Days to conduct Final Acceptance Testing and review the implemented Goods and/or Services to ensure they conform with the Acceptance Criteria.

8.3 The Supplier agrees to assist the Participating Authority, as requested, in the performance of such testing and review and to cooperate with **[other suppliers and employees of the Participating Authority]** in the conducting of such testing and review.

9 Implementation and Acceptance Testing of Goods and Services – Final Acceptance Criteria ☐

9.1 The Supplier is required to issue Test Certificates as detailed within Appendix 1 of the Specification.

9.2 If any of the **[Pre-Acceptance Criteria]; [Provisional Acceptance Criteria]; and/or the [Final Acceptance Criteria]** are not met in their entirety following completion of the relevant testing the Participating Authority may nevertheless at its discretion elect to provide its signature of any test certificates subject to rectification of any minor faults or errors. In such circumstances, the Supplier shall use all reasonable endeavours to rectify such faults or errors within the time period as specified in the applicable test certificate or, if no time period is so specified, within fourteen (14) days of the date of signature of the relevant test certificate.

10 Locations subject to lease and/or licence ☐

10.1 The provision of access by the Participating Authority to the Supplier to the Premises and Locations shall be subject to the lease and/or license appended at Appendix 5.

11 Change Control Process ☐

11.1 Any changes to this Contract, including to the Services and Goods, may only be agreed in accordance with the Change Control Process set out in Appendix 3.

12 TUPE ☐

12.1 Notwithstanding Key Provision 8 of the Contract Terms and Conditions, the Parties agree that the commencement of the provision of the Services under this Contract shall give rise to a relevant transfer as defined in TUPE and the provisions of Appendix 8 shall apply to such transfer.

13 Termination Sum ☐

13.1 Should the Participating Authority terminate this Contract in accordance with this Clause 13, then the Participating Authority shall pay to the Supplier the termination sum calculated in accordance with Appendix 7.

14 Step In Rights ☐

14.1 If the Supplier is unable to provide the Services, then the Participating Authority shall be entitled to exercise Step In Rights set out in Appendix 6.

15 Key Performance Indicators ☒

15.1 The KPI's and Service Credits applicable to the Contract are detailed in Appendix 10.

16 End User License Agreement (EULA) ☒

16.1 The Participating Authority is licensed to use such Goods and Service(s) in accordance with the EULA applicable to those Goods, and by entering into these Terms and any Contract pursuant to them, the Participating Authority agrees to enter into and comply with the terms of such EULA(s).

16.2 The EULA applicable to the relevant Software Product, as stipulated by the manufacturer of the Goods is appended at Appendix 9.

16.3 The Supplier hereby grants (or shall procure the grant in the case of rights owned by third parties) to the Participating Authority, and the Participating Authority hereby accepts from the Supplier, a [world-wide, non-exclusive, irrevocable, perpetual, transferrable, license] to use and exploit the Goods and the Consumables. No fee shall be payable for the grant of this license other than the charges detailed in Appendix 2 (Contract Pricing). The foregoing license(s) shall be: [Concurrent User License]

16.4 The Supplier shall deliver all Software electronically.

17 Intellectual Property Rights ☐

17.1 The Supplier confirms and agrees that [all/ specific detail on] Intellectual Property Rights in and to the deliverables, material and any other output developed by the Supplier as part of the Services in accordance with the Specification, shall be owned by the Participating Authority. The Supplier hereby assigns with full title guarantee by way of present and future assignment all Intellectual Property Rights in and to such deliverables, material and other outputs. The Supplier shall ensure that all Staff assign any Intellectual Property Rights they may have in and to such deliverables, material and other outputs to the Supplier to give effect to this Clause and that such Staff absolutely and irrevocably waive their moral rights in relation to such deliverables, material and other outputs. This Clause shall continue notwithstanding the expiry or earlier termination of this Contract.

18 Social Value ☒

18.1 The Supplier will comply with the Social Value detailed within Appendix 12.

19 New Technologies ☐

19.1 During the Term, if any new product or new technology related to the Goods (each a "**New Technology Product**") becomes available from the Supplier and it is obligatory for the Participating Authority to accept such Goods, the Supplier will replace the existing Goods pursuant to the Framework Agreement and shall not be permitted to increase the Contract Price in respect of such product(s).

19.2 In the event that the Participating Authorities are given the option to replace existing Goods supplied pursuant to the Contract with a New Technology Product (i.e., such replacement is not obligatory), the Supplier may increase the Contract Price to reflect that the Participating Authorities have opted to purchase such New Technology Product(s) provided always that such replacement produce and increased price is in accordance with Law. In the case of the latter situation, the Supplier shall provide the Authority and the Participating Authorities with full details of the New Technology Product and the additional costs (if any) associated with such products (applying discounts comparable to those applicable to the existing Goods under the Framework Agreement) in order for the Participating Authorities to make an informed decision as to whether to replace the existing Goods with the New Technology Product(s).

19.3 The Supplier shall notify the Authority and the Participating Authorities in writing of such at least thirty (30) days prior to the New Technology Products being made available for purchase through commercial/public release.

19.4 During the Term, if the Authority is notified of a New Technology Product pursuant to Clause 19.3 the Authority may request and the Supplier shall agree to supply the New Technology Product solely to the Participating Authority for a period of [insert number], prior to such New Technology Product being made available for purchase through commercial/public release.

20 Pricing for Goods ☐

20.1 The Prices detailed within Appendix 2 are inclusive of the costs of packaging, insurance and carriage of the Goods.

20.2 Arrangement for export shall be made by the Supplier and any applicable freight and shipping expenses, tariffs, customs, duties, or fees shall be paid for by the Supplier.

20.3 The Supplier shall use best endeavours to assist the Participating Authority with any issues with a carrier or insurer for mis-delivery or loss or damage to Goods. The Supplier will pay any excess costs due to failure to follow applicable shipping instructions.

Annex 3 - Optional Terms for Software and Services

1. **Pricing for Services – Total Cost** ☒

1.1 The total Price for the Services shall be the amount set out in the Call off Contract.

2. **Pricing for Services – Instalments** ☐

2.1 The total Price shall be paid to the Supplier in instalments. The Supplier shall invoice the Participating Authority for the charges that are then payable as detailed in Appendix 2.

3 Pricing for Services – Maintenance and Support Services ☒

3.1 The Supplier shall invoice the fees for Maintenance and Support Services in advance annually.

4 Pricing for Services – Fixed Pricing ☐

4.1 Any fixed price and daily rate contained in the Participating Authority Schedule excludes: the cost of hotel, subsistence, travelling and any other ancillary expenses reasonably and properly incurred by members of the supplier's team in connection with the Services.

4.2 The cost of any materials and the cost of services reasonably and properly provided by third parties and required by the Supplier for the supply of the Services. Such expenses, materials and third-party services shall be invoiced by the Supplier at cost. The Supplier shall obtain the Participating Authority's written approval before incurring any such expense, material or service exceeding £**[insert].**

4.3 The Supplier shall obtain and maintain at its own expense any and all necessary consents, licenses, approvals and permits required for its provision of Services.

5 Implementation of Software ☒

5.1 If the implemented Goods and Services function with any Errors or fail to conform to the Acceptance Criteria as defined in the applicable Contract, the Participating Authority may reject such Goods or Services, and the related implementation services, by providing the Supplier with written notice specifying such Errors and/or failures.

5.2 Upon receipt of such notice referred to above, the Supplier shall correct all such Errors and/or failures as soon as practicable, but no later than [**please see KPI's]** from the date of Participating Authority's notice of rejection.

5.3 Upon receipt of such notice above the Supplier shall provide a remediation plan and schedule. Upon receipt of the remediation plan, the Participating Authority shall then have, at a minimum, **[10]** Business Days to test and review the corrected Goods and Services according to the Acceptance Criteria.

5.4 If the Supplier is unable to correct the Error(s), the Participating Authority may elect to [terminate the Contract, without prejudice to any other rights to which it is entitled or resubmit a notice of rejection to the Supplier for a second and final opportunity to correct such Error and/or failure].

5.5 For avoidance of doubt, any approval by the Participating Authority under this section shall not limit or alleviate or absolve the Supplier's responsibilities, representations, warranties, and obligations otherwise set forth in the Contract

6 Software Errors ☒

6.1 The Supplier shall promptly notify the Participating Authority of any material defects or malfunctions in the Vendor Software or Documentation as soon as reasonably practicable. The Supplier, its agents or Sub-contractors shall promptly correct, or have corrected, any material defects or malfunctions in the Vendor Software or Documentation discovered and provide the Participating Authority with corrected copies of same, without additional charge.

6.2 The Suppliers obligation hereunder will not be deemed to affect any other liability that it may have to the Participating Authority.

6.3 If the Participating Authority notifies the Supplier in writing that the Vendor Software has failed to perform in accordance with the applicable Documentation or to conform to Vendors representations and warranties, the Supplier shall, **[at its own cost and expense]** and within **7 working** days of such written notice, either correct each deficiency or provide the Participating Authority with a plan, for its approval, for correcting the deficiency.

7 Supplier Quality Commitments for Software Licenses ☒

7.1 The Supplier shall use reasonable endeavours to ensure that all Vendor Software licensed pursuant to this Contract:

- shall operate in conformance with the Documentation.
- will not disable or interfere with any other process, system or technology of Participating Authority
- complies with applicable Laws.

8 Supplier Quality Commitments for Software – Dispute Resolution ☒

8.1 The Supplier, its agents or Sub-contractors shall not remove, alter, disable, corrupt, or interfere with the Vendor Software for purposes of preventing the Participating Authority from using the Vendor Software, or otherwise intentionally rendering the Vendor Software inoperable as the result of any dispute under this Contract. In the event of dispute or delayed payment, either party may refer the dispute in accordance with Clause 22 (Dispute Resolution).

9 Supplier Quality Commitments for Software-as-a-Service ☒

9.1 The Supplier shall use reasonable endeavours to ensure that the Software-as-a-Service (SaaS) shall be performed:

- in a timely, high quality and professional manner, using only qualified agents.
- in conformance with generally acceptable industry standards.
- in compliance with all applicable Laws.
- in compliance with any accreditation standards applicable to the Supplier.

10 Maintenance and Support Services for Software ☒

10.1 The Supplier shall provide to the Participating Authority, without additional charge, copies of the Documentation revised to reflect any Improvement to the Vendor Software made during the Maintenance and Support Services period.

10.2 At the Participating Authority's request, the Supplier shall prepare and submit to the Participating Authority a detailed report describing all of the Maintenance and Support Services provided to it by the Supplier under the Contract during the [prior year or quarter].

10.3 The Supplier shall provide, [at its own expense], [Telephone, email, and internet-based] support for advice and assistance to the Participating Authority on the use of Vendor

Software, (**namely: basic information and instructions, including assistance with the general use of the Vendor Software, optimisation of the available functions, installation of the Vendor Software, research problems reported by the Participating Authority, and any expected future modifications, new releases, fixes, updates, revisions, enhancements, and changes "Improvements" to the Vendor Software.**

10.4 The Supplier will provide the Maintenance and Support Services for **[all releases]** on the Vendor's support matrix, but in no event less than the most current release of the Vendor Software. These Maintenance and Support Services are **[free of charge/ priced as per Appendix 2]**

11 Maintenance and Support Services for Software - Remote dial-in access ☒

11.1 The Participating Authority shall maintain a direct telephone line or Virtual Private Network (VPN)connection to assist the Supplier and its Sub-contractors in providing remote dial-in access. The Participating Authority shall use reasonable efforts to inform the Supplier of any username and password changes pertaining to any VPN connections.

12 Deliverables created pursuant to the terms of this Contract ☒

12.1 Deliverables are deemed to be the Participating Authority's Confidential Information hereunder and, except as permitted herein, shall not be used or disclosed by the Supplier for any purpose without the Participating Authority's express written approval.

12.2 The Supplier shall obtain the Participating Authority's prior written consent before incorporating any third-party materials into any Deliverables. If Deliverables contain materials the Supplier or others previously developed, patented or copyrighted and which were not developed as a result of providing the Goods and Services under this Contract, the Supplier hereby grants the Participating Authority and the Participating Authority hereby accepts, an irrevocable, perpetual, world-wide, royalty-free transferrable license to use, copy, modify, distribute, display, perform, import, manufacture, have made, and sublicense such materials for the purpose of exercising the Participating Authority's rights, title and interest in the Deliverable, to the extent Supplier has the right to grant such a licence.

12.3 The Supplier agrees that if, in the course of performing, delivering or otherwise providing the Services, the Supplier or its agents and Sub-contractors incorporate into any Deliverable or otherwise use any Prior Inventions, then the Supplier will provide the Participating Authority with prior written notice and the Participating Authority is hereby granted a royalty-free, perpetual, irrevocable, transferrable, sub-licenseable, worldwide license to make, have made, use,

import, offer for sale, sell, reproduce, distribute, modify, adapt, prepare derivative works of, display, perform, and otherwise exploit such Prior Inventions, without restriction for any and all purposes to the extent reasonably required in connection with the Participating Authority's receipt or use of the Services or Deliverables. All other rights in and to the Prior Inventions are expressly reserved by the Supplier.

13 **New Releases of Software** ☒

13.1 During the term of this Contract, the Supplier agrees it shall provide the Participating Authority with [all] new releases of software which are modifications to the Vendor Software, fixes, updates, revisions, improvements, enhancements, and other changes

("**Improvements**") to such Vendor Software that are generally offered to the Supplier's customers.

13.2 The Participating Authority may, at its sole discretion, approve or reject any Improvement. Any Improvement approved by the Participating Authority shall be deemed to be Vendor Software and subject to the terms and conditions of the EULA Contract.

14 Subsequent Versions of Software ☒

14.1 The Supplier will make available to the Participating Authority all subsequent versions "**Subsequent Versions**" of the Vendor Software. Subsequent Versions are modifications or upgrades to the Vendor Software that add significant functionality and may be supplied for an additional cost. The Supplier will send any release notes related to Improvements or Subsequent Versions in the manner and to the location specified by Participating Authority in the Specification (Appendix 1).

15 Software–as–a –Service (SaaS) ☒

15.1 The Supplier will provide all SaaS Services (including, without limitation, configuration and implementation of the SaaS Services, [and consulting services]) subject to the Contract, as necessary to enable the Participating Authority and its authorised users to access and use the Software, the SaaS Services, and all associated data and information (including, without limitation, the Data) over a secure web-enabled connection, in accordance with the Participating Authority's requirements, Specifications, and minimum acceptable service levels.

15.2 As part of the SaaS Services, the Supplier shall:

- procure and maintain the infrastructure (including hardware, Software, networks, connectivity, security, tools and other resources) as necessary to securely host the SaaS application and deliver the SaaS Services.
- ensure that the SaaS Application and all Data shall be maintained on secure servers located in Data Centres.

15.3 The Supplier and/or its Sub-contractor shall ensure that fully redundant mirrored image copies of the SaaS Application, the related infrastructure and Data simultaneously reside in a backup server(s) (capable of operating as a hot site with no fail-over elapsed time), physically located in another Data Centre **("Back-Up Data Centre)**. The Supplier shall ensure its system backups and shall procure that its Sub-contractor's system backups will ensure that the Data is encrypted in transit and at rest (including at the Back-Up Data Centre).

15.4 The Supplier shall ensure and shall procure that its Sub-contractor will ensure that all Data is logically segregated from other data, including the Supplier's other Participating Authorities' data, and shall secure and restrict access to Data solely to the Participating Authority and its Authorized Users and ensure that the SaaS Services are otherwise provided in compliance with any applicable data processing agreement, and all applicable Laws.

15.5 The Supplier has provided the name and locations of its hosting site(s) in Appendix 1 (Specification) of the Call off Contract and the Data Protection Protocol.

15.6 In the event of any change of the location(s) of the Data Center(s), the Supplier shall provide the Participating Authority with prior written notice of said change and disclose the address of the new Data Center.

15.7 The Supplier shall provide the SaaS Services at least in accordance with the Minimum Agreed Service Levels (MASL), detailed within Appendix 1 (Specification) of the Call off Contract.

The Supplier shall provide the Participating Authority with all necessary technical changes and any configuration and implementation procedures required for the Participating Authority to access and use the SaaS Services.

16 Data Ownership ☒

16.1 The Supplier acknowledge and agree that the Participating Authority is the exclusive owner of all right, title and interest in and to the Data. The Supplier may only use Data in strict performance of its obligations under the Contract, unless otherwise agreed in writing with the Participating Authority.

17 Participating Authority Obligations (SaaS) ☒

17.1 The Participating Authority shall not:

- disclose, disseminate, reproduce or publish any portion of the SaaS Services in any manner or permit the same;
- use the SaaS Services to create derivative products or other derivative works; or
- disassemble, decompile, manipulate or reverse engineer any portion of the SaaS Services.

[List any other relevant restrictions imposed by the third-party SaaS supplier.]