Crown Commercial Service

G-Cloud 12 Call-Off Contract

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

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	128079019470580
Call-Off Contract reference	Prj_7534
Call-Off Contract title	Financial Transaction Processing (Middle Office) 2022-2025
Call-Off Contract description	HMCTS require a range of data handling, processing, reconciliation, banking and MI related services as detailed in Schedule 1 (Specification) to support the Court services.
Start date	1st January 2023
Expiry date	31st December 2024
Call-Off Contract value	£15,700,000 (Fifteen Million, Seven Hundred Thousand Pounds)
Charging method	Purchase Order

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

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

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

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

From the Buyer	HM Courts and Tribunals Service Ministry of Justice 102 Petty France London SW1H 9AJ

To the Supplier	Liberata UK Limited 5th Floor, Knollys House 17 Addiscombe Road Croydon CR0 6SR Company number: 01238274
Together the 'Parties'	

Principal contact details

For the Buyer:

Contractual:

Title: Commercial Manager, Ministry of Justice

Name: [REDACTED

Email: [REDACTED]

Phone: [REDACTED]

Operational:

Title: Head of Financial Accounts, HMCTS

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

For the Supplier:

Title: Head of Automation Services, Liberata UK Limited

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **1st January 2023** and is valid for **24 months**. [The date and number of days or months is subject to clause 1.2 in Part B below.]
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1).
Extension period	This Call-off Contract can be extended by the Buyer for 2 period(s) of up to 12 months each, by giving the Supplier **3 months** written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: ● Lot 2: Cloud software
G-Cloud services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below: Cloud software in the category Other accounting and finance services, where the supplier is not a reseller, where user support is available by phone, where users can access the service through a web browser interface, where usage metrics are provided through real-time dashboards and regular reports, where the service is connected to the Public Services Network (PSN), where data protection between buyer and supplier networks includes a private network or public sector network, where data storage and processing locations include the United Kingdom and where suppliers are prepared to make sure their staff have Security Clearance (SC)

	Tender Form and Response reproduced in full at Schedule 1 Annex 3 of this Call-off Contract.
Additional Services	Transition Services, as required to deliver the offboarding activities in line with the Exit Strategy.
Location	The services shall be performed primarily at the supplier's premises: Unit B, Fountain Court St Mellons Business Park Cardiff CF3 0FB Elements of the services may be provided at other locations within the UK.
Quality standards	The quality standards required for this Call-Off Contract are ISO-22301 - Business Continuity Management Systems; ISO-27001 – Information Security Management System; ISO 27002 - Information technology – Security techniques – Code of practice for information security controls ISO-9001 - Quality Management Systems; and OHSAS 18001 - Health and Safety Management. BPSS or BS7858 or equivalent Non-Police Personnel Vetting level 2 (NPPV2) - only applies to staff accessing Pentip
Technical standards:	Cyber Essentials Certificate
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are detailed in Schedule 1 (Specification).

Onboarding	N/A
Offboarding	The Exit plan and transition services as defined in Clause 21.
Collaboration agreement	N/A
Limit on Parties' liability	The annual total liability of either Party for all Property defaults will not exceed £1,000,000. The annual total liability for Buyer Data defaults will not exceed £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance	The insurance(s) required will be: • a minimum insurance period of 6 years following the expiration or Ending of this Call-off Contract • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law. • professional indemnity cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher the Buyer requires (and as required by Law)

	In respect of the Supplier held Professional Indemnity cover, the requirement for a minimum limit of indemnity of £1,000,000 for each individual claim. It is agreed that this may be substituted, at the Supplier's request, with the view of reverting to standard G-Cloud indemnity levels when possible, by the following: The supplier (i) shall hold professional indemnity insurance in the aggregate to £20 million; (ii) shall utilise its cash reserves in the event of its professional indemnity insurance cover having been exhausted; (iii) has and shall maintain at all relevant times a parent company guarantee with Outsourcing Inc., Japan; (iv) shall utilise its existing Cyber insurance insofar as this may afford cover for an individual claim made in connection with the Services; (v) shall continue to monitor the insurance market and shall obtain Per Claim professional indemnity insurance cover as soon as this is available on reasonable commercial terms; (vi) shall notify the buyer, in the monthly reporting, of any professional indemnity claim against Liberata during the reporting period; (vii) shall notify the buyer, in the monthly reporting, of any reduction in the aggregate insurance available; and (b) that the waiver be subject to formal review by the Authority and the supplier at six-monthly intervals, where at each formal review the Authority reserves the right to revoke the waiver at its sole discretion.
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 60 consecutive days.
Audit	The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: **<u>What will happen during the Framework Agreement's Term</u>** 7.4 The Supplier will maintain full and accurate records and accounts, using Good Industry Practice and generally accepted accounting principles, of the: 7.4.1 operation of the Framework Agreement and the Call-Off Contracts entered into with Buyers

7.4.2 Services provided under any Call-Off Contracts (including any Subcontracts)

7.4.3 amounts paid by each Buyer under the Call-Off Contracts

What will happen when the Framework Agreement Ends

7.5 The Supplier will provide a completed self-audit certificate (Schedule 2) to CCS within 3 months of the expiry or Ending of this Framework Agreement.

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

7.6.1 7 years after the date of Ending or expiry of this Framework Agreement

7.6.2 7 years after the date of Ending or expiry of the last Call-Off Contract to expire or End

7.6.3 another date agreed between the Parties

7.7 During the timeframes highlighted in clause 7.6, the Supplier will maintain:

7.7.1 commercial records of the Charges and costs (including Subcontractors' costs) and any variations to them, including proposed variations

7.7.2 books of accounts for this Framework Agreement and all Call-Off Contracts

7.7.3 MI Reports

7.7.4 access to its published accounts and trading entity information

7.7.5 proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Framework Agreement

7.7.6 records of its delivery performance under each Call-Off Contract, including that of its Subcontractors

What will happen during an audit or inspection

7.8 CCS 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 CCS's control.

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

7.9.1 provide audit information without delay

7.9.2 provide all audit information within scope and give auditors access to Supplier Staff

7.10 The Supplier will allow the representatives of CCS, Buyers 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:

7.10.1 the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement)

7.10.2 any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call-Off Contract only

7.10.3 the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier

7.10.4 any other aspect of the delivery of the Services including to review compliance with any legislation

7.10.5 the accuracy and completeness of any MI delivered or required by the Framework Agreement

7.10.6 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

7.10.7 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 CCS its reasonable Audit costs if it reveals:

	7.11.1 an underpayment by the Supplier to CCS in excess of 5% of the total Management Charge due in any monthly reporting and accounting period 7.11.2 a Material Breach 7.12 CCS can End this Framework Agreement under Section 5 (Ending and suspension of a Supplier's appointment) for Material Breach if either 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 granting access/availability of office space to host meetings when required.
Buyer's equipment	[REDACTED]

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners: [REDACTED]

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is via Purchase Order.
Payment profile	The payment profile for this Call-Off 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	PDF invoices emailed to the shared service centre APinvoices-CTS-U@gov.sscl.com.
Invoice information required	All invoices must include Purchase Order reference.
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	The total value of this Call-Off Contract is £15,700,000 (Fifteen Million, Seven Hundred Thousand Pounds)
Call-Off Contract charges	The breakdown of the Charges is detailed in Schedule 2 of this Call-off Contract.

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the Implementation Plan, exit and offboarding plans and milestones required.
Guarantee	This Call-Off Contract is conditional on the Supplier providing a Guarantee to the Buyer.

Warranties, representations	In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants and represents to the Buyer that it will enter into a parent company guarantee in the form set out in Schedule 5 hereunder.
Supplemental requirements in addition to the Call-Off terms	Within the scope of the Call-Off Contract, the Supplier will: N/A
Alternative clauses	These Alternative Clauses, which have been selected from Schedule 4, will apply: N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	Within the scope of the Call-Off Contract, the Supplier will: **<u>Remedies in the Event of Inadequate Performance</u>** The Authority shall be entitled to take all reasonable steps to investigate any performance issues or complaint it receives regarding: a) the standard of Services; b) the manner in which any Services have been supplied; c) the manner in which work has been performed; d) the Equipment, materials or procedures the Contractor uses; or e) any other matter connected with the performance of the Contractor's obligations under the Contract, including Key Performance Indicators and Service Levels. In the event that the Authority reasonably believes that there has been a Default of the Contract by the Contractor, irrespective of whether the Default is a Material Breach, then the Authority may at no additional cost to the Authority and at the Contractor's own cost, without prejudice to its rights and remedies under the Contract or otherwise do any of the following:

a) request in writing that the Contractor remedies the Default within a period specified by the Authority; or

b) require the Contractor to submit a Performance Improvement Plan within ten (10) Working Days (or such other period as notified by the Authority to the Contractor) of a written request from the Authority:

i. The Performance Improvement Plan shall include details of why the Default has occurred, how the Default will be remedied and the date by which the Default will be remedied.

ii. The following actions in this clause shall apply in respect of the Performance Improvement Plan:

1. The Authority shall either approve or reject in writing the Performance Improvement Plan within ten (10) Working Days (or such other period as notified by the Authority to the Contractor) of its receipt pursuant to this clause

2. If the Authority rejects the Performance Improvement Plan it shall set out the reasons and the Contractor shall address all such reasons in a revised Performance Improvement Plan, which it shall submit to the Authority within a further period of ten (10) Working Days (or such other period as notified by the Authority to the Contractor) (“Revised Performance Improvement Plan”) of its receipt of the Authority's reasons.

3. If the Performance Improvement Plan or Revised Performance Improvement Plan (as appropriate) is agreed the Contractor shall immediately start work on the actions set out in the Performance Improvement Plan or Revised Performance Improvement Plan (as appropriate).

If, despite the measures taken under this clause, the Revised Performance Improvement Plan cannot be agreed within a period of ten (10) Working Days (or such other period as notified by the Authority to the Contractor) of receipt by the Contractor of the Authority’s reasons in respect of the Performance Improvement Plan then the Authority may:- (i) end the Performance Improvement Plan process and refer the matter for resolution by the dispute

	resolution processes included in the G Cloud 12 Framework; or (ii) deem the Default as a Material Breach and exercise its rights under clause 18.5.
Public Services Network (PSN)	The Public Services Network (PSN) is the government's secure network. If the G-Cloud Services are to be delivered over PSN this should be detailed here: [REDACTED]
Personal Data and Data Subjects	As detailed in Schedule 7

1. Formation of contract

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

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

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

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

2. Background to the agreement

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

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

Signed	Liberata UK Limited	Ministry of Justice
Name		

Title		
Signature		
Date		

Schedule 1: Services

1. Services to be provided

The Services below are referenced in accordance with the section references within the HMCTS Middle Office Service Specification v2.1.2 for Financial Transaction Processing (Middle Office) services.

3.1 Magistrates Banking Returns (MBR)
3.2 Magistrates BACS Processes
3.3 Cash Management
3.4 Deposits Including Bail
3.5 Penalty Payments
3.6 Roadside Deposits
3.7 Magistrates' Domestic and Foreign Payments and Drafts (BACS, Faster Payment, CHAPS)
3.8 UK Border Agency (UKBA) Fee Awards
3.9 Centralised Attachment of Earnings Payment System (CAPS)
3.10 Crown and County Court Banking and Accounting Returns (BAR)
3.11Printed Cheque Schedules from the County Court Case Management System (CaseMan)
3.12 Payments and Secure Cheque Printing
3.13 Creation & Management of Customer Accounts
3.14 Direct Debit Facility (DD)
3.15 Fee Account (Payment by Account or PbA)
3.16 Bulk Scanning
3.17 Data Received from Online Services
3.18 Immigration and Asylum Chamber Fees (IAC)
3.19 Fee refunds
3.20 Money Claims Online (MCOL) and Possession Claims Online (PCOL)
3.21 Rolls Building Online Fees (CE file)
3.22 Magistrates Travel and Subsistence (T&S)
3.23 Banking Stationery
3.24 Banking Administration and Other Banking Services
3.25 Cash Delivery and Collection
3.26 Consolidated Funds Extra Receipts (CFER) & 3.26 Inter-Department Transfers (IDT)
3.27 Funding Process
3.28 Chargebacks
3.29 Payments and Secure Cheque Printing
3.30 Data Storage and Management information
3.31 Helpdesk and Support

Schedule 2: Call-Off Contract charges

1. Charges for Services

This section details Liberata's pricing proposal submitted as part of the tender process for HMCTS Financial Transaction Processing (Middle Office) 2022-24 services through G-Cloud 12.

The pricing schedule below is referenced in accordance with the HMCTS Middle Office Service Specification v2.1.2 for Financial Transaction Processing (Middle Office) services.

The calculated total contract value for all services over the initial period of the new contract 1st January 2023 to 31st December 2024 is £15.7M, this is based on an analysis of 2021 volumes, which have been annualised for the purpose of this calculation and includes estimated project costs of [REDACTED]

Fixed Prices in the below table represent the fixed monthly charge. Variable prices represent the per transaction charge. All prices exclude VAT.

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

[REDACTED]

2. Charges Rate Card

Liberata's rate card for projects and change requests is detailed below, prices exclude VAT:

[REDACTED]

3. Service Credits

3.1 Service Credits shall be calculated by reference to the number of Service Points accrued in any one Service Period pursuant to the provisions of Annex B of the Schedule 1 (Service Levels).

3.2 For each Service Period:

(a) the Service Points accrued shall be converted to a percentage deduction from the Service Charges for the relevant Service Period on the basis of one point equating to a 1% deduction in the Service Charges; and

(b) the total Service Credits applicable for the Service Period shall be calculated in accordance with the following formula:

$$SC = TSP \times x \times AC$$

where:

SC	is the total Service Credits for the relevant Service Period;
TSP	is the total Service Points that have accrued for the relevant Service Period;
x	is 1%; and
AC	is the total Services Charges payable for the relevant Service Period (prior to deduction of applicable Service Credits).

3.3 The liability of the Supplier in respect of Service Credits shall be subject to a Service Credit Cap provided that, for the avoidance of doubt, the operation of the Service Credit Cap shall not affect the continued accrual of Service Points in excess of such financial limit in accordance with the provisions of Annex B of the Schedule 1 (Service Levels).

3.4 Service Credits are a reduction of the Service Charges payable in respect of the relevant Services to reflect the reduced value of the Services actually received and are stated exclusive of VAT.

3.5 Service Credits shall be shown as a deduction from the amount due from the Authority to the Supplier in the invoice for the Service Period immediately succeeding the Service Period to which they relate.

Part B: Terms and conditions

1. Call-Off Contract start date and length

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

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

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

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

2. Incorporation of terms

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

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

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

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

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

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

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

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

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

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

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

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

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

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

5. Due diligence

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

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

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

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

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

6. Business continuity and disaster recovery

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

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

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

7. Payment, VAT and Call-Off Contract charges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Insurance

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

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

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

9.3.1 a broker's verification of insurance

9.3.2 receipts for the insurance premium

9.3.3 evidence of payment of the latest premiums due

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

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

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

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

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

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

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

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

10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity 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 Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.

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

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

11.4 The Supplier must promptly inform the Buyer if it 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:

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

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

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

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

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

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

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

11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.7.3 other material provided by the Buyer necessary for the Services

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

12. Protection of information

12.1 The Supplier must:

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

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

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

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

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

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

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

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

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

13. Buyer data

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

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

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

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

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

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

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

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

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

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

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

13.6.6 buyer requirements in respect of AI ethical standards

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

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer

Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

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

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

14. Standards and quality

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

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

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

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

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

15. Open source

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

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

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 20 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

21.1 The Supplier must provide an exit plan at mobilisation that ensures continuity of service and the Supplier will follow it.

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

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

21.4 The Supplier must ensure that the 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 exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the 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 exit plan ensures that:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control. This may require more than one copy of the data at different times if deemed necessary. One copy of the data to be provided free of charge and subsequent copies may be chargeable at day rates provided in Schedule 2.

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

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

23. Force majeure

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

24. Liability

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

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

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

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

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

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

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably

possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

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

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

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

29.6.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer 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:

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 3: Collaboration agreement

(NOT USED)

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 8.12 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for 'FoIA/Freedom of Information Act' to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.2.

2.1.6 References to "tort" will be replaced with "delict" throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988

- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996
- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004
- Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

a. persons of different religious beliefs or political opinions
b. men and women or married and unmarried persons
c. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
d. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
e. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
f. persons of different ages
g. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

a. the issue of written instructions to staff and other relevant persons

b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters
d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or
B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier's compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer's cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.

In respect of Liberata UK Limited a G-Cloud 12 Parent Company Guarantee has been agreed and signed by Outsourcing Inc. – refer to separate signed deed.

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but 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 Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.

End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party 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 Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans

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

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trademarks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
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 G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.

Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: 1 induce that person to perform improperly a relevant function or activity 2 reward that person for improper performance of a relevant function or activity 3 commit any offence: a. under the Bribery Act 2010 b. under legislation creating offences concerning Fraud c. at common Law concerning Fraud d. committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.

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

Schedule 7: GDPR Information

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

Annex 1: Processing Personal Data

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

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

Descriptions	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: Names Addresses Bank details Email addresses
Duration of the Processing	Contract Duration 1st Jan 2023 to 31st Dec 2024 with 2 possible 12-month extensions
Nature and purposes of the Processing	**Magistrates T&S Claims via the Magistrates Claims Portal** Name, address, bank account details, email address An automated process where the Magistrates T&S portal interfaces with the suppliers' payment processing system to initiate payment.

	Pentip Refund Process Name, address, bank account details An automated process with little or no manual intervention. **Magistrates Bacs Payment** Name, bank account details An automated process using the supplier's Bacs Portal that requires no manual intervention. **Bail Deposits** Offender name, offence description, depositor name, depositor address, depositor bank account details Currently managed by completion of forms that are emailed to the supplier. **Fee Repayment/Refunds** Name, address to enable refund by cheque. Name, bank account details for refund by Bacs. **Roadside Deposits** Offender name, offender address To enable deposit to be created and refunds in the event of an overpayment, information is also used to match the deposit to the case court extract once the matter has been dealt with by the Court. **Domestic and Foreign Payments** Name, bank account details To enable international payments by bank transfer, information is provided by a form completed by the business. **Centralised Attachment of Earnings** Payer name, address to enable payment by cheque Payer name, bank account details for payment by Bacs Details are provided by an interface to enable payments to be made. **Cheque Printing** Recipient name, address Details provided from printed cheque schedules from CaseMan or via the Payment Portal/BAR return. **Creation/Management of Customer Accounts** A credit check (CC) is undertaken before an account is set up. The CC requires the following: applicant legal name, Law Society/Limited Company

	registration number, registered office address, number of years trading, trading name if different, billing details, a signed declaration. Additional information such as bank statements and annual accounts may be required for the credit check process. Information is provided by the customer. **Manage Direct Debits Payments from Professional Users** Recipient name, address, bank account details to pay by Bacs. Details provided by the customer as part of the application process. **Bulk Scanning for Civil matters** Name, bank account details For customers paying by cheque these are received by API and stored in the supplier's database. **UKBA** Name, bank account details for payment by Bacs. Data is pulled from ARIA to enable payment.
Type of Personal Data	Names Addresses Bank details Email Addresses
Categories of Data Subject	HMCTS Customers Judiciary Legal professionals Users of online payment services website Users of the application website
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	To comply with current HMCTS data retention requirements.

Schedule 8: Supplier’s Commercially Sensitive Information

1 Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge that the Authority may have to disclose Information in or relating to the Contract following a Request for Information pursuant to clause D4 (Freedom of Information).

2 In this Schedule 4 the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.

3 Where possible the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule 4 applies.

4 Without prejudice to the Authority’s obligation to disclose Information in accordance with the FOIA and the EIR, the Authority will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

SUPPLIER’S COMMERCIALLY SENSITIVE INFORMATION	DATE	DURATION OF CONFIDENTIALITY
Technical Clarification document Section T-01 Details of the key leadership, the CIO and details of their experience	22/03/2022	The life of the contract
Technical Clarification document Section T-06	22/03/2022	The life of the contract
Technical Clarification document Section T-07	22/03/2022	The life of the contract
Technical Clarification document Section T-08 Current and future service specification	22/03/2022	The life of the contract
Technical Clarification document Section T-10 Details of future improvements	22/03/2022	The life of the contract
Commercial Clarification document Section C-01	22/03/2022	The life of the contract
Commercial Clarification document Section C-02	22/03/2022	The life of the contract
Charges Template	22/03/2022	The life of the contract
Financial Viability Risk Assessment	22/03/2022	The life of the contract

Schedule 9: Supplier's Carbon Reduction Footprint

Carbon Reduction Plan – Liberata UK Limited – 7 March 2022

Commitment to Achieving Net Zero

Liberata UK Limited is committed to achieving Net Zero emissions by 2040.

Baseline Emissions Footprint

Baseline emissions are a record of the greenhouse gases that have been produced in the past and were produced prior to the introduction of any strategies to reduce emissions. Baseline emissions are the reference point against which emissions reduction can be measured.

Table 1 : Baseline year emissions

Baseline Year: 2020	
Additional Details relating to the Baseline Emissions calculations.	
The Baseline carbon footprint has been calculated using the energy consumptions and emissions from the sources included in our SECR report for the year ending December 2020. Those scope 1, 2 and 3 emissions required in addition by the Carbon Reduction Plan Guidance were then calculated and added to the SECR totals. The year 2020 is the earliest period for which reliable collated data are available but comprises a period when company operations were untypically constrained, by Covid-related influences, and as a result the baseline carbon footprint is also untypically low. While we remain committed to achieving net-zero by the stated date, it is likely that progress toward that target may, initially at least, be hesitant. If, and when, operations return to more normal levels we may adopt a more typical period to calculate a revised baseline and target progress trajectory against which to report progress.	
Baseline year emissions: Creation of an initial baseline.	
EMISSIONS	**TOTAL (tCO_2e)**
Scope 1	221.1
Scope 2	222.3
Scope 3 **(Included Sources)**	55.5

Total Emissions	499.0

Current Emissions Reporting

Table 2 : Reporting year emissions

Reporting Year: 2021	
EMISSIONS	**TOTAL (tCO_2e)**
Scope 1	223.1
Scope 2	190.6
Scope 3 **(Included Sources)**	55.0
Total Emissions	468.7 (-6.1% of Baseline)

Year-on-Year Comparison of Emissions by Source

The figures below illustrates the relative percentages of total emissions by source for the current reporting year compared with those for the baseline year, and help to illustrate which sources represent the greatest changes in emissions when compared with the baseline year.

Note that the calculations for each year, and in particular for 2021, incorporate a significant proportion of estimated data. Although these estimations are considered acceptably robust for the present purpose, it is to be hoped that improved data acquisition procedures will improve the accuracy of the calculations in subsequent years.

Figure 1: Carbon Emissions by source 2020

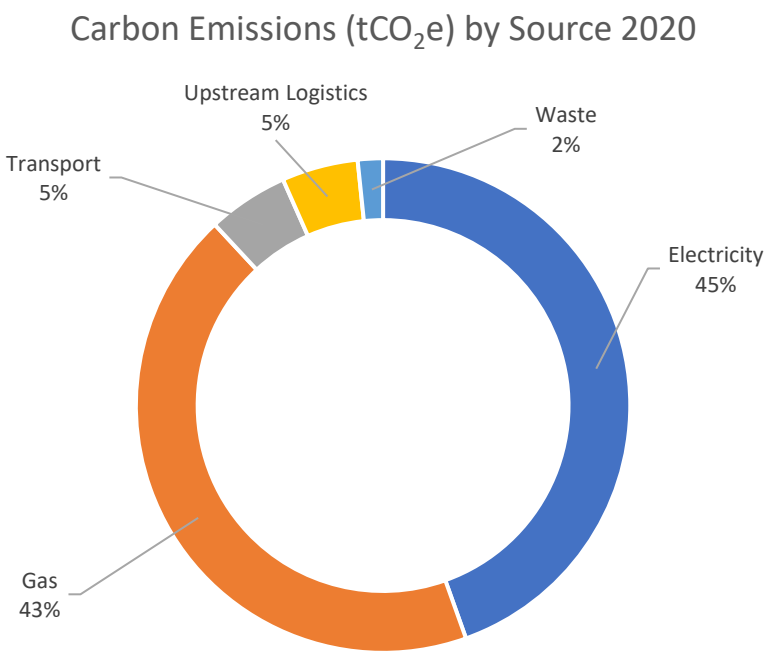
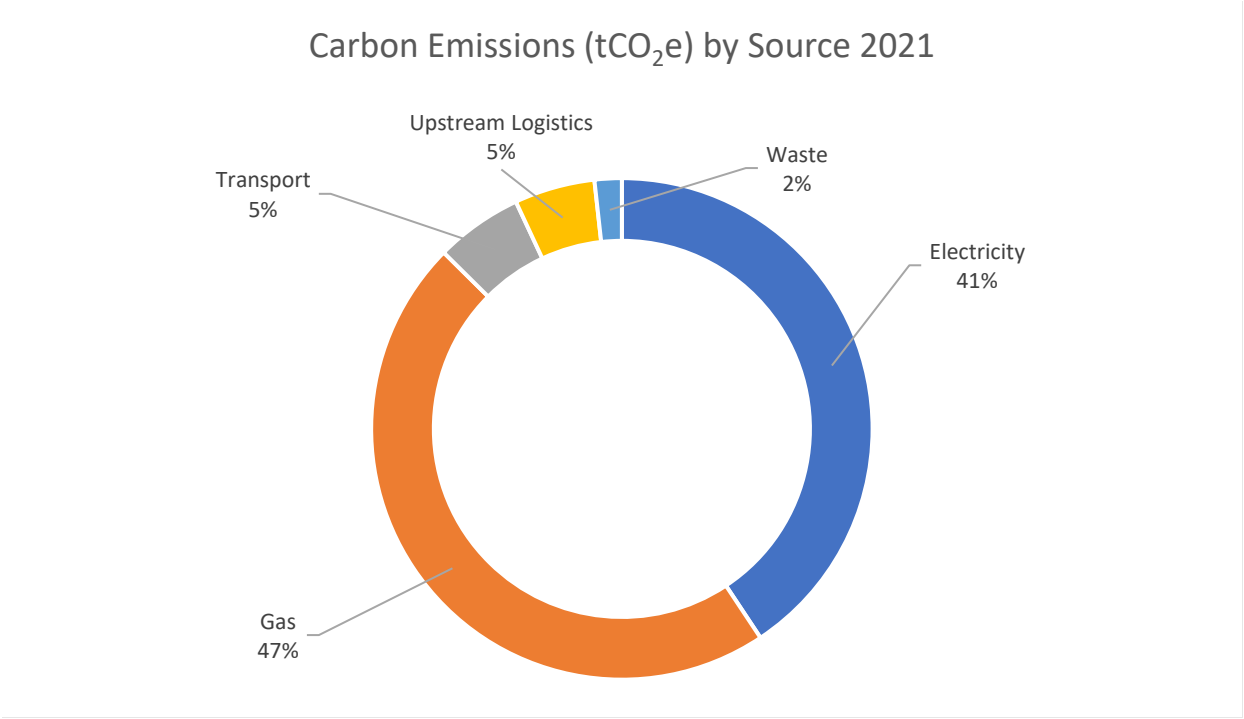


Figure 2: Carbon Emissions by source 2021



Emissions Reduction Targets

In order to continue our progress to achieving Net Zero, we have adopted the following carbon reduction targets:

- Achieve a 100% reduction of direct carbon dioxide equivalent (CO_2e) emissions by 2040.

We project that carbon emissions will decrease over the next five years to 345.4 tCO2e by 2026. This is a reduction of 31% compared with the 2020 baseline.

Progress against these targets can be seen in the graph below:

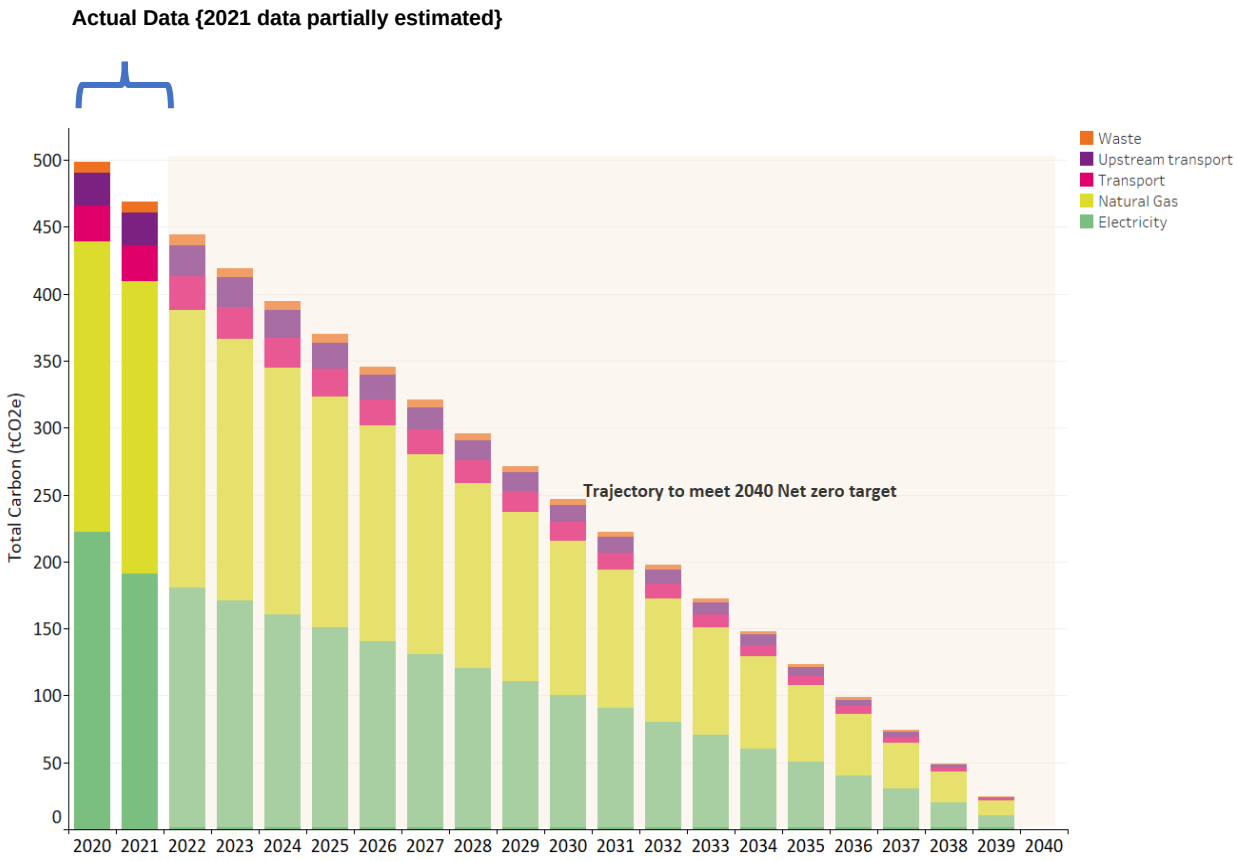


Figure 3: Total Carbon Emissions 2020-2040

Carbon Reduction Projects

Completed carbon reduction initiatives

The following environmental management measures and projects have been completed or implemented since the 2020 baseline.

- Office Lighting - Automatic movement sensor lighting installed.
- Use of office electrical equipment e.g. copiers, printers PCs, kitchen equipment - Employee awareness of personal control measures. Copiers/printers automatically go into sleep mode when not in use. Other office equipment switched off after use.
- Hot water - Use of energy efficient water heater in kitchens (point of use boiler). Regularly serviced and descaled. Regular weekly monitoring.
- Air Conditioning - Regular servicing and maintenance of the air conditioning. Local control of BMS system per floor to optimise efficiency.
- Working towards ISO 14001 – implementation delayed due to Covid.

The carbon emission reduction achieved by these schemes is estimated to be to 37.4 tCO2e, a 7.5% reduction against the 2020 baseline. This is not, however, fully reflected in the year-on-year comparison since the baseline reporting period corresponds to a period when company operations were temporarily constrained. The measures will remain in effect when performing the contract and the savings should become apparent if and when a baseline is adopted which represents a more typical operating period.

Pending carbon reduction initiatives

In the future we hope to implement further measures such as:

- Full implementation of ISO 14001
- Procurement of energy supplies from renewable sources
- Decarbonisation of heating systems
- Increased reuse and recycling of consumables.
- Increased co-location of data services to low carbon centres

Declaration and Sign Off

This Carbon Reduction Plan has been completed in accordance with PPN 06/21 and associated guidance and reporting standard for Carbon Reduction Plans.

Emissions have been reported and recorded in accordance with the published reporting standard for Carbon Reduction Plans and the GHG Reporting Protocol corporate standard[1] and uses the appropriate Government emission conversion factors for greenhouse gas company reporting[2].

Scope 1 and Scope 2 emissions have been reported in accordance with SECR requirements for non-quoted companies, and the required subset of Scope 3 emissions have been reported in accordance with
the published reporting standard for Carbon Reduction Plans and the Corporate Value Chain (Scope 3) Standard[3]. Note than in respect of the requirement to report emissions relating to downstream transportation and distribution, this company has no significant physical output and thus has no downstream transportation. This category of emissions has thus been omitted from Figure 1.

This Carbon Reduction Plan has been reviewed and approved by the Board of Directors of Liberata UK Limited.

Signed:

Charles Bruin, CEO

7 March 2022

[1] https://ghgprotocol.org/corporate-standard
[2] https://www.gov.uk/government/collections/government-conversion-factors-for-company-reporting
[3] https://ghgprotocol.org/standards/scope-3-standard

Annex A – DETAILED SECURITY REQUIREMENTS

Contents

1. GENERAL

1.1 The requirements in this Annex A build upon and extend the security requirements that can be found in the G-Cloud framework and call-off contract. Within this document references to “The customer” refer to the Ministry of Justice (MoJ) and its executive agency HMCTS.

2. Industry based security certification and best practices

2.1 The supplier shall hold ISO 27001:2013 certification issued by a UKAS registered certification body for the system(s) used for the solution and all related procedures or be prepared to commence the certification process within 6 months of contract signing. If it is not possible for the supplier, the reasons for this must be disclosed and discussed with the customer for resolution.

2.2 The supplier shall be certified to Cyber Essentials Plus or be prepared to commence certification within 3 months of contract signing. If it is not possible for the supplier, the reasons for this must be disclosed and discussed with the customer for resolution.

3. HMCTS policies, processes and procedures

3.1 The supplier shall supply the customer with a high-level design (solution blueprint) of the solution that has been baselined and agreed with the HMCTS security team. The design shall include how the security requirements of the contract/specification will be met.

3.2 The supplier shall provide a single point of contact for digital security and one for asset security .

3.3 The supplier shall provide a decommissioning approach document, at least 3 months ahead of the first planned decommissioning activity, detailing the decommissioning and disposal methodology for approval by the customer.

3.4 The supplier shall ensure that all supplier and sub-contractor staff who have access to personal data, including staff in their supply chain if appropriate, undergo a session of information risk awareness training on induction and annually thereafter.

3.5 The supplier shall produce and maintain an accurate inventory of information, system, hardware (where applicable) and software assets used to deliver the services (the “Information Asset Database” and the “Equipment Asset Database” and together with the “Asset Databases”).

3.6 The supplier shall ensure that all changes to services impacting IT security apply the agreed change procedure and take account of the latest Security Aspects Letter (SAL).

3.7 Supplier support staff shall be located within the UK . Support staff can be located outside the UK with the agreement of the Commercial Contract Manager

3.8 The supplier is not permitted to extract/export any data outside of this service specification, without written consent from the customer, as advised by designated HMCTS staff.

3.9 Data in any non-production environment shall not contain live data without prior approval from the customer, as advised by designated HMCTS staff.

3.10 The supplier shall ensure, and provide evidence to the customer, that all security requirements – functional and non-functional – applicable to the contractor, will flow down in the supply chain and will apply to all sub-contractors, Partners, and suppliers that participate in this contract.

4. Information Security Management System (ISMS) and Security Management Plan (SMP)

4.1 The Supplier shall provide an ISMS to the Customer, the ISMS shall cover the secure reception, processing, storage and dissemination of Customer information within controlled physical and electronic environments. This ISMS shall meet the requirements of ISO/IEC 27001:2013.
In accordance with ISO/IEC 27001:2013 Annex A, the ISMS shall cover the 14 security areas related to the Services.
The ISMS shall also:

- be developed to protect all aspects of the Services and all processes associated with the provision of the Services, including to support Sites, the ICT Environment, information and data.
- meet the relevant standards in ISO/IEC 27001 (Information Security Management) and ISO/IEC27002 (Information Technology – Security Techniques).
- be supported by appropriate security standards, guidance and policies applicable to the Services provided to the Customer.

4.2 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies related to the ISMS set out in this contract, the Supplier shall immediately notify the Customer's Security Representative of such inconsistency who shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

4.3 The supplier shall prepare, develop, maintain and deliver to the customer for approval a complete and up to date Security Management Plan (SMP) covering all services delivered under this contract, within 20 working days after the commencement date. The Security Management Plan shall be structured in accordance with ISO27001 and ISO27002 and conform to the general obligations set out in the HMG IA standards. A link to the preferred template is provided here:
https://tools.hmcts.net/confluence/display/ISMS/SMP+Template?src=contextnavpagetreemode

4.4 The SMP shall:

- identify the necessary delegated organisational roles defined for those responsible for delivering and overseeing the SMP.
- detail the Supplier approach and processes for delivering the Services using Sub-Contractors and third parties authorised by the Customer.

4.5 The ISMS and SMP shall be reviewed and updated by the Supplier as necessary to reflect:

- emerging changes in Good Industry Practice.
- any change or proposed change to Services and/or associated processes.
- any changes to the Customer's security policies as notified by the Customer.
- any new perceived or changed security threats.
- any reasonable change in requirement requested by the Customer.

4.6 The Supplier shall provide the Customer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and SMP at no additional cost to the Customer. The results of the review shall include, without limitation:

- updates to the risk assessments.
- proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security.
- suggested improvements including in measuring the effectiveness of controls.

4.7 Subject to the requirements of this contract, any change which the Supplier proposes to make to the ISMS or SMP shall be subject to the Variation Procedure and shall not be implemented until Approved by the Customer.

4.8 The Customer may, where it is reasonable to do so, approve and require changes or amendments to the ISMS or SMP to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of the Contract.

5. Technical vulnerability management

5.1 The supplier shall provide evidence of penetration testing on all the applications within the system within the last six months. The supplier shall demonstrate that no critical or high vulnerabilities exist and that any medium or low vulnerabilities are being addressed.

5.2 The supplier shall supply full ITHC (CREST or CHECK certified) results of the system and a remedial action plan for any vulnerabilities uncovered by the ITHC.

5.3 Any vulnerabilities uncovered by an ITHC or further testing shall be resolved within the following periods. Critical - one week, High - two weeks, Medium and low - four weeks.

5.4 The supplier shall apply a patch immediately if the infrastructure for which they are responsible suffers from a vulnerability that is being exploited elsewhere.

5.5 The Supplier shall:

- conduct security tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the SMP.

- scope, design and implement security tests to minimise the impact on the delivery of the Services. The Customer shall be entitled to send a representative to witness the conduct of a security test.
- agree in advance with the Customer the acceptance criteria, date, timing, content and conduct of such security tests. The Customer shall not unreasonably withhold such agreement.
- provide the Customer with the results of such security tests (in a form Approved by the Customer) as soon as practicable but not more than 10 Working Days after each security test.

5.6 Where any security test carried out pursuant to this contract reveals any actual or potential breach of security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Customer of any changes to the ISMS and to the SMP (and the implementation thereof) which the Supplier proposes to make to correct such failure or weakness.

5.7 If any repeat security test carried out reveals an actual or potential breach of security exploiting the same root cause failure as uncovered in a previous test, such circumstance shall constitute a material default of this Agreement.

6. Secure configuration and access control

6.1 The system shall respond to changes to the role of a user(s) within the HMCTS IDAM (SSO IdP), within the minimum time possible (maximum 30 minutes).

6.2 Authentication and role-based access control (multi factor for manager's access), constraining the permissions of individual users to those necessary for least privilege shall be used.

6.3 It shall be possible to manage user permissions at a group and team level, as well as by individual user.

6.4 The supplier shall ensure segregation of duties by privileged users of the services, to ensure separation of request, approval and processing stages for account creation, changes to user permissions, account deletion, access to and processing of Protective Monitoring logs.

6.5 The system shall allow a user to be designated as a local administrator so that they can then create further accounts within their organisation.

6.6 The supplier shall ensure that the service limits all inbound and outbound traffic to only those sources/destinations and protocols required for the service to function, typically achieved using a boundary device, such as a Firewall.

6.7 The supplier shall verify all hardware (including virtual) and software configurations against unauthorised changes at least once during any period of twelve months. Evidence of the verification and its results will need to be examined.

6.8 The system shall perform a spam filtering function, phishing filtering function, malware filtering function - where applicable - to the solution (e.g., email handling or file uploads).

6.9 The system shall ensure that data is encrypted by default, whether at rest within the infrastructure, in transit within the infrastructure or in transit between the infrastructure and another environment. Deprecated ciphers must not be used.

6.10 Enforce access control through use of MFA, security attributes and enforcing the 'need to know' principle. Dual authorisation must also be used to conduct sensitive system changes.

6.11 Implement host-based protection such as host firewalls and host-based intrusion detection.

6.12 Use encryption to protect information. Encryption mechanisms should include Secure key management and storage.

6.13 Application Programming Interfaces (API) – All APIs should be protected using good practice security controls such as, authentication, integrity checking, encryption and limited data exposure, etc. All third-party interfaces should be covered by any MoU or other type of agreement, must comply with current GDPR legislation

6.14 End User Devices

- Authority Data shall, wherever possible, be held and accessed electronically in the ICT Environment on secure premises or via devices (incl. laptops) with secure remote access such that data can be viewed and amended over the internet/ intranet without being permanently stored on the remote devise, using products meeting the FIPS 140-3 standard or equivalent. Data will not be held and accessed on removable media (including removable discs, CD-ROMs, USB memory sticks, PDAs and media card formats) without Approval. Data received in paper format will be stored in a secure manner on site and not removed from site without permission.
- The right to transfer Authority Data to a remote device should be carefully considered and strictly limited to ensure that it is only provided where absolutely necessary and shall be subject to monitoring by the Supplier and Authority.
- Unless otherwise Approved, when Authority Data resides on a removable or physically uncontrolled device, it shall be:
    - the minimum amount that is necessary to achieve the intended purpose and should be anonymised if possible.
    - stored in an encrypted form meeting the FIPS 140-3 standard or equivalent and using a product or system component which has been formally assured through a recognised certification process of Certified Cyber Security Consultancy Guide (CESG) to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("**CPA**") or equivalent, unless otherwise Approved.
    - protected by an authentication mechanism, such as a password; and
    - have up to date software patches, anti-virus software and other applicable security controls to meet the requirements of this Schedule 8.
- Devices used to access or manage Authority Data shall be under the management authority of the Supplier and have a minimum set of security policy configurations enforced. Unless otherwise Approved, all Supplier devices shall satisfy the security requirements set out in the national cyber security centre (https://www.ncsc.gov.uk/collection/device-security-guidance)
- Where the NCSC Guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. If the

Supplier wishes to deviate from the NCSC Guidance, this should be agreed in writing with the Authority on a case-by-case basis.

6.15 Data Storage, Processing, Management, Transfer and Destruction

- The Parties recognise the need for Authority Data to be safeguarded and for compliance with the Data Protection Legislation. To that end, the Supplier shall inform the Authority the location within the United Kingdom where Authority Data is stored, processed and managed. The import and export of Authority Data from the Supplier System must be strictly controlled and recorded.
- The supplier shall ensure proactive monitoring is in place to ensure storage facilities, is sufficient to meet the requirement as set out in the specification.
- The Supplier shall inform the Authority of any changes to the location within the United Kingdom where Authority Data is stored, processed and managed and shall not transmit, store, process or manage Authority Data outside of the United Kingdom without Approval which shall not be unreasonably withheld or delayed provided that the transmission, storage, processing and management of Authority Data offshore is within:
    - the European Economic Area ("**EEA**"); or
    - another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into, which have been defined as adequate by the European Commission.
- The Supplier shall ensure that any electronic transfer of Authority Data:
    - protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data.
    - maintains the integrity of the Authority Data during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data; and
    - prevents the repudiation of receipt through accounting and auditing.
- The Supplier shall:
    - protect Authority Data, including Personal Data, whose release or loss could cause harm or distress to individuals and ensure that this is handled as if it were confidential while it is stored and/or processed.
    - ensure that OFFICIAL-SENSITIVE information, including Personal Data is encrypted in transit and when at rest when stored away from the Supplier's controlled environment.
    - on demand, provide the Authority with all Authority Data in an agreed open format.
    - have documented processes to guarantee availability of Authority Data if it stops trading.
    - securely destroy all media that has held Authority Data at the end of life of that media in accordance with any requirements in the Contract and, in the absence of any such requirements, in accordance with Good Industry Practice.
    - securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority.
    - ensure that all material used for storage of Confidential Information is subject to controlled disposal and the Supplier shall:
        - destroy paper records containing Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and

        - dispose of electronic media that was used for the processing or storage of Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.
    - The supplier shall maintain and evidence operating procedures in relation to:
        - Document storage including off-site and third-party arrangements
        - Document access
        - Scanning
        - Indexing
        - Retrieval
        - System administration
        - Backup
        - Archiving

6.16 Networking

- Any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of Public Sector Network ("**PSN**") compliant encrypted networking services or equivalent unless none are available in which case the Supplier shall agree the solution with the Authority.
- The Authority requires that the configuration and use of all networking equipment in relation to the provision of the Services, including equipment that is located in secure physical locations, is at least compliant with Good Industry Practice.
- The Supplier shall ensure that the ICT Environment (to the extent this is within the control of the Supplier) contains controls to maintain separation between the PSN and internet connections if used.

7. Communication security

7.1 All connectivity to the service, including for management purposes, should have the following controls:

- The monitoring and control of remote access methods.
- Ensuring all remote access methods are encrypted.
- Enabling the capability to rapidly disconnect a user from accessing an information system, and/or revoking further remote access.

7.2 Classify system connections and apply restrictions to external systems and public networks.

7.3 To protect the network against malicious actors and code, implement the following security controls:

- Vulnerability scanning tools.
- Intrusion detection systems.
- Signature and non-signature-based detection of malicious code or behaviour.
- Software patching and updates.
- Detection of unauthorised commands.
- Tools for real-time analysis of logs.
- Detection of indicators of compromise.

8. Security monitoring

8.1 The supplier shall have a protective monitoring policy to assist in identifying security incidents quickly and to provide the customer with information that will assist in initiating the incident response policy as early as possible.

8.2 The system shall report security critical events to the customer's and supplier's Security Information and Event Management (SIEM) solution. The user shall be prevented from tampering with the reporting of events from the device. The logs shall be retained for 90 days minimum, except where legally they shall be kept longer in line with HMCTS retention policies.

9. Decommissioning and disposal

9.1 Decommissioning, disposal or sanitisation and destruction of infrastructure and data shall be carried out in line with NCSC guidance.

9.2 The Supplier shall provide a HLD for decommissioning and disposal for approval by the Customer. For individual decommissioning activities shall provide a detailed LLD for approval by the Customer.

10. Confidentiality and security classifications

10.1 The Supplier shall be informed by the customer via the Security aspect letter of the data classification that the supplier needs to maintain, it is probable customer information provided to the Supplier under the Services, whether in paper or electronic form, shall be classified as OFFICIAL. Additionally, the Customer will identify to the Supplier certain sensitive information as OFFICIAL SENSITIVE which shall require additional security protection.

10.2 Where the Supplier is requested to manage Customer Data designated as OFFICIAL SENSITIVE additional security measures, generally procedural or personnel, must be applied to reinforce the principle of Need to Know. The Supplier shall manage this under enhanced security requirements, using the following principles (as a minimum):

- store Customer Data within an environment which is not shared (i.e., Customer Data must be in a locked and secure separate area which does not contain records from any other client of the Supplier).
- only enable access to Customer Data from permanent, contract, associate, agency and sub-contract staff who are authorised on a need to know basis. The Customer shall advise if any personnel need to hold an appropriate current UK Government national security vetting.
- allow external access to pre-authorised Customer personnel only.
- immediately upon Supplier notification, report to the Customer any incidents involving theft, loss or inappropriate access to Customer Data (using such reporting mechanism as defined by the ISMS).

11. Incident management

11.1 The Customer and the Supplier shall notify the other upon becoming aware of any breach of security or any potential or attempted breach of security (including

throughout the supply chain) in accordance with the agreed security incident management process as defined by the ISMS or SMP.

11.2 Upon becoming aware of an actual, potential or attempted breach of security, the Supplier shall immediately take all reasonable steps (which shall include any action or changes reasonably required by the Customer) necessary to:

- minimise the extent of actual or potential harm caused by any breach of security.
- fully cooperate with the Customer to support notifying other third parties.
- remedy such breach of security or any potential or attempted breach of security to protect the integrity of the Customer Property and/or ISMS or SMP to the extent that this is within the Supplier's control.
- apply a tested mitigation against any such breach of security or attempted breach of security. Provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Services the Customer must be advised before implementation so that appropriate direction can be given.
- prevent a further breach of security or any potential or attempted breach of security in the future exploiting the same root cause failure.
- supply any requested data to the Customer (or the Computer Emergency Response Team for the Government ('GovCertUK') on the Customer's request within 48 hours and without charge (where such requests are reasonably related to a possible incident or compromise).
- as soon as reasonably practicable, provide to the Customer full details (using the reporting mechanism defined by the ISMS) of the breach of security or the potential or attempted breach of security, including a root cause analysis where required by the Customer.

12. Security audit

12.1 The Customer shall provide reasonable notice to the Supplier prior to any Security Audit of the Services provided, the ISMS and SMP. The Customer shall try to ensure that such Security Audits are requested no more than twice each Call Off Contract Year. Notwithstanding the foregoing, such Audits may be required:

- more frequently in the event of a serious security situation.
- immediately in case of a security related incident.

12.2 The Supplier shall provide to the Auditors access to all information necessary to perform the Security Audit. The Supplier shall also assist the Customer's staff and/or auditors in testing the Customer Data, files and programs, including installing and running audit software.

12.3 To assist with any Security Audit, the Supplier shall always:

- ensure that they keep electronic records of their compliance with the provisions of this contract, to provide sufficient evidence to the Customer (if required).
- make available to the Customer these records to assist the Customer with satisfying itself (or others, as may be required) that the Supplier is delivering the Services to accord with these requirements.

12.4 If, because of a Security Audit as described in this contract, the Supplier is found to be noncompliant then the Supplier shall, at its own expense, undertake those actions

required to achieve the necessary compliance and shall reimburse in full the costs incurred by the Customer in obtaining such Audit.

12.5 Upon reasonable notice provided by the Customer, the Supplier shall provide the Customer and such auditors and inspectors as the Customer may designate in writing, access to Supplier's (and any Sub-contractor's) Premises as may be necessary for the Customer (or its agents or representatives) to perform any Security Audit.

- Access will only be required at reasonable hours.
- The access to Supplier's Premises shall include the use of Supplier's office furnishings, telephone and Wi-Fi services, utilities and office-related equipment and duplicating services or any other such facilities that Auditors and inspectors may reasonably require to perform the Security Audits described.

13. Supply chain security management

13.1 Supplier to demonstrate how they would provide supply chain management. Supporting systems shall be hosted and, unless agreed otherwise with the customer, supported in the UK on an ISO27001 or NCSC compliant system with proper separation from other customers and with adequate malware and virus protection.

13.2 Supplier must have a procurement and third-party support processes supply chain security policy which covers (at a minimum):

- How information is shared with, or is accessible to, third party suppliers and the supply chains.
- How procurement processes place security requirements on third party suppliers.
- How security risks from third-party suppliers are managed.
- How the management of supply chain compliance with security requirements are managed.
- How hardware and software used in the service are verified as genuine and has not been tampered with.

13.3 Supplier must provide a list of sub-contractors where applicable.

14. Business continuity and disaster recovery

14.1 The Supplier shall prepare and deliver to the Customer for the Customer's written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:

- ensure continuity of the business processes and operations supported by the Services following any failure or disruption.
- the recovery of the Services in the event of a Disaster.

14.2 The BCDR Plan shall have a section detailing general principles and requirements which shall:

- set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other.
- provide details of how the invocation of any element of the BCDR Plan may impact upon the operation of the provision of the Services and any services provided to the Customer by a Related Supplier.

- contain an obligation upon the Supplier to liaise with the Customer and (at the Customer's request) any Related Suppliers with respect to issues concerning business continuity and disaster recovery where applicable.
- detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the Customer and any of its other Related Supplier in each case as notified to the Supplier by the Customer.
- contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels.
- contain a risk analysis, including:
- failure or disruption scenarios and assessments and estimates of frequency of occurrence.
- identification of any single points of failure within the provision of Services and processes for managing the risks arising.
- identification of risks arising from the interaction of the provision of Services and with the services provided by a Related Supplier.
- a business impact analysis (detailing the impact on business processes and operations) of anticipated failures or disruptions.
- provide for documentation of processes, including business processes, and procedures.
- set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-Contractors) and for the Customer.
- identify the procedures for reverting to "normal service".
- set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity.
- identify the responsibilities (if any) that the Customer has agreed it will assume in the event of the invocation of the BCDR Plan.
- provide for the provision of technical advice and assistance to key contacts at the Customer as notified by the Customer from time to time to inform decisions in support of the Customer's business continuity plans.

14.3 The BCDR Plan shall be designed to ensure that:

- the Services are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan.
- the adverse impact of any Disaster, service failure, or disruption on the operations of the Customer is minimal as far as reasonably possible.
- that repeat running of transactions must not cause duplication
- it complies with the relevant provisions of ISO/IEC 27002 and all other industry standards from time to time in force.
- there is a process for the management of disaster recovery testing detailed in the BCDR Plan
- the system is designed to avoid single point of failure

14.4 The Supplier shall not be entitled to any relief from its obligations under the Service Levels or to any increase in the Charges to the extent that a Disaster occurs because of any breach by the Supplier of this Contract.

14.5 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the provision of Services remain supported and to ensure continuity of the business operations

supported by the Services including, unless the Customer expressly states otherwise in writing:

- the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Services; and
- the steps to be taken by the Supplier upon resumption of the provision of Services to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

14.6 The Disaster Recovery Plan shall be:

- designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Customer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- invoked only upon the occurrence of a Disaster.

14.7 The Disaster Recovery Plan shall include the following:

- the technical design and build specification of the Disaster Recovery System.
- details of the procedures and processes to be put in place by the Supplier in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including, but not limited to, the following:
    - Trigger points for the initiation of the disaster recovery plan
    - data centre and disaster recovery site audits.
    - backup methodology and details of the Supplier's approach to data back-up and data verification.
    - Restoration timelines for all services
    - identification of all potential disaster scenarios.
    - risk analysis.
    - documentation of processes and procedures.
    - hardware configuration details.
    - network planning including details of all relevant data networks and communication links.
    - invocation rules.
    - Service recovery procedures.
    - steps to be taken upon resumption of the provision of Services to address any prevailing effect of the failure or disruption of the provision of Services.
- any applicable Service Levels with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Service Levels in respect of the provision of other Services during any period of invocation of the Disaster Recovery Plan.
- details of how the Supplier shall ensure compliance with security standards and ensure that compliance is maintained for any period during which the Disaster Recovery Plan is invoked.
- access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule.
- testing and management arrangements.

14.8 The Supplier shall review the BCDR Plan (and the risk analysis on which it is based):

- on a regular basis and as a minimum once every six (6) months.

- within three calendar months of the BCDR Plan (or any part) having been invoked.
- where the Customer requests any additional reviews (over and above those provided for in this Contract) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Customer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total cost payable by the Customer for the Customer's approval. The costs of both Parties of any such additional reviews shall be met by the Customer except that the Supplier shall not be entitled to charge the Customer for any costs that it may incur above any estimate without the Customer's prior written approval.

14.9 Each review of the BCDR Plan pursuant to this Contract shall be a review of the procedures and methodologies set out in the BCDR Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within the period required by the BCDR Plan or, if no such period is required, within such period as the Customer shall reasonably require. The Supplier shall, within twenty (20) working days of the conclusion of each such review of the BCDR Plan, provide to the Customer a report (a "Review Report") setting out:

- the findings of the review.
- any changes in the risk profile associated with the provision of Services.
- the Supplier's proposals (the "Supplier's Proposals") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any goods, services or systems provided by a third party.

14.10 Following receipt of the Review Report and the Supplier's Proposals, the Customer shall:

- review and comment on the Review Report and the Supplier's Proposals as soon as reasonably practicable.
- notify the Supplier in writing that it approves or rejects the Review Report and the Supplier's Proposals no later than twenty (20) working days after the date on which they are first delivered to the Customer.

14.11 If the Customer rejects the Review Report and/or the Supplier's Proposals:

- the Customer shall inform the Supplier in writing of its reasons for its rejection.
- the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Customer's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Customer for the Customer's approval within twenty (20) working days of the date of the Customer's notice of rejection.

14.12 The Supplier shall as soon as reasonably practicable after receiving the Customer's approval of the Supplier's Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

14.13 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Customer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Customer.

15. Back up

15.1 The Supplier shall perform full daily secure back-ups of all HMCTS Data and systems used to administer work associated with this contract and shall ensure that up-to-date back-ups are stored off-site at an Approved location in accordance with any BCDR Plan or otherwise. The Supplier shall ensure that such back-ups are available to the Customer (or to such other person as the Customer may direct) at all times, upon request.

15.2 Automated backup, archive, and retrieval processes must be in place, including documentation, prior to go live

15.3 Automated backup / recovery procedures must consider, system growth and specify such things as what is to be backed up, size, type of backup and ensure compatibility with existing infrastructure.

15.4 All key software, configuration settings, databases, flat files and standing data will be backed up should there be a need to reload or restore them

15.5 Capability should exist to restore only the data item that is required. E.g., An entire database should not have to be restored to recover a single file

15.6 The Supplier will ensure that back-up systems are tested at least once per annum to ensure data reliability, integrity and that back up data can be restored allowing users to access as normal. Results should be shared with the Security Working group as part of Contract performance management reviews.

15.7 Backup schedules are to be kept for a length of time to be agreed with HMCTS.

ANNEX B

SERVICE LEVELS

Part A: Service Levels and Service Credits

1. SERVICE LEVELS
2. SERVICE POINTS
3. REPEAT SERVICE LEVEL THRESHOLD FAILURES AND RELATED SERVICE LEVEL FAILURES
4. PERMITTED MAINTENANCE
5. SERVICE CREDITS

Part B: Service Level Performance Monitoring

1. PERFORMANCE MONITORING AND PERFORMANCE REVIEW
2. PERFORMANCE VERIFICATION

Part C: Service Level and KPI Tables

1. Key Service Levels
2. Subsidiary Service Levels
3. Key Performance Indicators

1 DEFINITIONS

1.1 In this Annex B, the following definitions shall apply:

"Available"	The IT Environment and/or the Services shall be Available when: (a) End Users are able to access and utilise all the functions of the Supplier System and/or the Services; and (b) the Supplier System is able to process the Authority Data and to provide any required reports within the timescales set out in the Services Description; and (c) all Service Levels other than Service Availability are above the Service Level Threshold.
"End User"	any person authorised by the Authority to use the IT Environment and/or the Services;
"Extended Service Hours"	Any period which is Service Hours for at least one of the Services
"Help Desk"	the single point of contact help desk set up and operated by the Supplier for the purposes of this Agreement;
"Key Performance Indicator"	the Key Performance Indicators set out in Section 3 of Part C
"Key Service Level"	the key Service Levels set out in Section 1 of Part C
"KPI Target"	the Key Performance Indicator performance targets set out in Section 3 of Part C
"KPI Target Failure"	a failure to meet the KPI Target in respect of a Key Performance Indicator
"Non-Available"	in relation to the IT Environment or the Services, that the IT Environment or the Services are not Available;
"Performance Failure"	a Service Level Failure or a KPI Target Failure;
"Permitted Maintenance"	has the meaning given in Section 2.6, (System Requirements) of Schedule 1 (Services);
"Repeat Service Level Threshold Failure"	has the meaning given in Section 3.1 of Part A;

"Service Availability"	has the meaning given in Section 2.7 of Part C
"Service Downtime"	any period of time during which any of the Services are not Available; and
"Service Charges"	the periodic payments made in accordance with Schedule 2 (*Call-Off Contract Charges*) in respect of the supply of the Operational Services;
"Service Credits"	credits payable by the Supplier due to the occurrence of 1 or more Service Level Failures, calculated in accordance with Section 3 of Schedule 2 (*Call-Off Contract Charges*)
"Service Credit Cap"	5% of the Charges applicable for the Service Period
"Service Downtime"	Any period of time during which any of the Services are not Available within the respective Service Hours for the individual service
"Service Hours"	The periods of time when services are due to be Available, as defined below: • Fee Account – 6am-8pm Monday to Friday and 9am-4pm Saturday and Sunday • Direct Debit System – 6am-8pm Monday to Friday and 9am-4pm Saturday and Sunday - • Magistrates T&S – 6am -11pm daily • All other Services – 8 am-6pm Monday to Friday
"Service Levels"	the Key Service Levels and the Subsidiary Service Levels;
"Service Level Failure"	a failure to meet the Target Performance Level in respect of a Key Service Level;
"Services"	any and all of the services to be provided by the Supplier under this Agreement, including those set out in Schedule 1 (*Services*);
"Service Level Performance Monitoring Report"	has the meaning given in Section 1.2 of Part B;
"Service Level Threshold"	shall be as set out against the relevant Key Performance Indicator in Section 1 of Part C

"Service Level Threshold Failure"	a failure to meet the Service Level Threshold in respect of a Key Service Level
"Service Period"	a calendar month, save that: (a) the first service period shall begin on the first Operational Service Commencement Date and shall expire at the end of the calendar month in which the first Operational Service Commencement Date falls; and (b) the final service period shall commence on the first day of the calendar month in which the Term expires or terminates and shall end on the expiry or termination of the Term;
"Service Points"	has the meaning given in Section 2 of Part A
"Subsidiary Service Level"	the subsidiary service levels set out in Section 2 of Part C
"Target Performance Level"	the minimum level of performance for a Key Service Level which is required by the Authority, as set out in Section 1 of Part C

PART A: SERVICE LEVELS AND SERVICE CREDITS

1 SERVICE LEVELS

1.1 Part C sets out the Key Service Levels, Subsidiary Service Levels and Key Performance Indicators which the Parties have agreed shall be used to measure the performance of the Services by the Supplier.

1.2 The Supplier shall monitor its performance against each of the Service Levels and Key Performance Indicators and shall send the Authority a monthly report detailing the level of service actually achieved in accordance with Part B.

1.3 Service Points, and therefore Service Credits, shall accrue for any Service Level Threshold Failure and shall be calculated in accordance with Paragraphs 2, 3 and 5.

2 SERVICE POINTS

2.1 If the level of performance of the Supplier during a Service Period achieves the Service Level Threshold in respect of a Key Service Level, no Service Points shall accrue to the Supplier in respect of that Key Service Level.

2.2 If the level of performance of the Supplier during a Service Period is below the Service Level Threshold in respect of a Key Service Level, a Service Point shall accrue to the Supplier in respect of that Key Service Level, unless the Service Level Threshold Failure is a Repeat Service Level Threshold Failure when the provisions of Paragraph 3.2 shall apply.

3 REPEAT SERVICE LEVEL THRESHOLD FAILURES AND RELATED SERVICE LEVEL FAILURES

Repeat Service Level Threshold Failures

3.1 If a Service Level Threshold Failure occurs in respect of the same Key Service Level in any two consecutive Service Periods, the second and any subsequent such Service Level Threshold Failure shall be a "**Repeat Service Level Threshold Failure**".

3.2 The number of Service Points that shall accrue to the Supplier in respect of a Service Level Threshold Failure that is a Repeat Service Level Threshold Failure is two.

Related KPI Failures

3.3 If a single failure causes two or more Key Service Levels to incur a Service Point, or Service Points, then the Supplier shall only incur Service Points for one of the Service Level Failures: In the event that the different Service Level Failures attract different numbers of Service Points then it shall be the Service Level Failure that attracts the most Service Points that is counted.

4 PERMITTED MAINTENANCE

4.1 The Supplier shall be allowed to book Service Downtime for Permitted Maintenance as agreed in writing with the Authority.

5 SERVICE CREDITS

5.1 Schedule 2 (*Charges*) sets out the mechanism by which Service Points shall be converted into Service Credits.

5.2 The Authority shall use the Service Level Performance Monitoring Reports provided pursuant to Part B, among other things, to verify the calculation and accuracy of the Service Credits (if any) applicable to each Service Period.

5.3 Service Credits are not an exclusive remedy to service failures.

PART B: SERVICE LEVEL PERFORMANCE MONITORING

1 PERFORMANCE MONITORING AND PERFORMANCE REVIEW

1.1 The Supplier shall include reporting of performance levels against Service Levels and Key Performance Indicators within the Specification, Section 2.1 (Governance and Contract reporting) and 1.2 below.

Service Level Performance Monitoring Report

1.2 The Service Level Performance Monitoring Report shall be in such format as agreed between the Parties from time to time and contain, as a minimum, the following information:

Information in respect of the Service Period just ended

(a) for each Key Service Level, Subsidiary Service Level and Key Performance Indicator, the actual performance achieved over the Service Period, and that achieved over the previous Service Periods during that calendar year;

(b) a summary of all Performance Failures that occurred during the Service Period;

(c) which Performance Failures remain outstanding and progress in resolving them;

(d) the status of any outstanding rectification plan processes, including:

(i) whether or not a rectification plan has been agreed; and

(ii) where a rectification plan has been agreed, a summary of the Supplier's progress in implementing that rectification plan;

(e) for any Repeat Service Level Threshold Failures, actions taken to resolve the underlying cause and prevent recurrence;

(f) the number of Service Points awarded in respect of each Service Level Threshold Failure;

(g) the Service Credits to be applied, indicating the Service Level Threshold Failure(s) to which the Service Credits relate;

(h) the conduct and performance of any agreed periodic tests that have occurred, such as the annual failover test of the Service Continuity Plan;

(i) relevant particulars of any aspects of the Supplier's performance which fail to meet the requirements of this Agreement;

(j) such other details as the Authority may reasonably require from time to time; and

Information in respect of previous Service Periods

(k) for each Service Level and Key Performance Indicator, a rolling total of the number of Performance Failures that have occurred over the previous Service Periods during that calendar year;

(l) the amount of Service Credits that have been incurred by the Supplier during that calendar year;

(m) the conduct and performance of any agreed periodic tests that have occurred in such Service Period such as the annual failover test of the Service Continuity Plan; and

Information in respect of the next Quarter

(n) any scheduled Service Downtime for Permitted Maintenance and Updates that has been agreed between the Authority and the Supplier for the next Quarter.

2 SERVICE LEVEL PERFORMANCE RECORDS

2.1 The Supplier shall keep appropriate documents and records (including Help Desk records, staff records, timesheets, training programmes, staff training records, goods received documentation, supplier accreditation records, complaints received etc) in relation to the Services being delivered. Without prejudice to the generality of the foregoing, the Supplier shall maintain accurate records of call histories for a minimum of 12 months and provide prompt access to such records to the Authority upon the Authority's request. The records and documents of the Supplier shall be available for inspection by the Authority and/or its nominee at any time and the Authority and/or its nominee may make copies of any such records and documents.

2.2 In addition to the requirement in Paragraph 2.1 to maintain appropriate documents and records, the Supplier shall provide to the Authority such supporting documentation as the Authority may reasonably require in order to verify the level of the performance of the Supplier both before and after each Operational Service Commencement Date and the calculations of the amount of Service Credits for any specified period.

PART C: SERVICE LEVEL AND KPI TABLES

The Key Service Levels and Subsidiary Service Levels that shall apply to the Services are set out below:

1 Key Service Levels

1.1 Definition

Ref.	Key Service Level	Description	Target Performance Level	Service Level Threshold
KSL-1	Posting Transactions	All transactions received are posted to the correct account Performance of SLA to be measured against: Subsidiary Performance Levels SSL1-1 to SSL1-9	98%	90%
KSL-2	Direct Debits	All direct debits are drawn to agreed timescales Performance of SLA to be measured against: Subsidiary Performance Levels SSL2-1 10 SSL2-09	99%	90%
KSL-3	Payments Out	All payments out are made to agreed timelines Performance of SLA to be measured against: Subsidiary Performance Levels SSL3-1 to SSL3-9	99%	90%
KSL-4	Account Reconciliations	All reconciliations completed to agreed timelines Performance of SLA to be measured against: Subsidiary Performance Levels SSL4-1to SSL4-11	99%	90%
KSL-5	Bank account management and reconciliations	All reconciliations completed to agreed timelines Performance of SLA to be measured against: Subsidiary Performance Levels SSL5-1 to SSL5-6	99%	90%
KSL-6	Customer Account Applications	Applications validated and processed to agreed timelines Performance of SLA to be measured against: Subsidiary Performance Levels SSL6-1 to SSL6-6	95%	90%
KSL-7	Service Availability	Services to be available in line with agreed specifications Performance of SLA to be measured against: Subsidiary Performance Level SSL7-1	98%	90%

KSL-8	Social Value - Tackling Economic Inequality	Number of people-hours of learning interventions per FTE in Wales over life of contract	140	140

1.2 Calculation of the Key Service Levels KSL-1 to KSL-6 and the Key Performance Indicators:

For each Key Service Level, or Key Performance Indicator, the calculation of the performance level achieved is as follows

$$value = \left(\left(\frac{\mathrm{C1}}{\mathrm{T1}}\right) + \left(\frac{\mathrm{C2}}{\mathrm{T2}}\right) + \left(\frac{\mathrm{C3}}{\mathrm{T3}}\right) + \left(\frac{\mathrm{C4}}{\mathrm{T4}}\right) \ldots . + \left(\frac{\mathrm{C}n}{\mathrm{T}n}\right)\right) / n$$

Where,

Cn = Number of transactions completed successfully, which means to the required quality and by the required target time as defined in Section 2 below.

Tn = Number of transactions due to be completed successfully.

n = Number of Subsidiary Service Levels that make up the Key Service Level, as defined in Section 2 below.

The measures for C1 to C9 include any transactions correctly completed on the measurement day that were due to be correctly completed on a previous but were not.

The measures for T1 to T9 include any transactions that were not correctly completed on a previous day and so are due to be correctly completed on the measurement day.

1.3 Calculation of the Key Service Level KSL-7:

This is as defined in section 2.7

1.4 Calculation of Key Service Level KSL-8

Calculation based on actual delivery hours per FTE of activities that demonstrate learning interventions under Model Assessment Criteria 2.2 of the Social Value Model:

MAC 2.2: Create employment and training opportunities particularly for those who face barriers to employment and/or who are located in deprived areas, and for people in industries with known skills shortages or in high growth sectors.

Sub-Criteria for MAC 2.2

- Support for the contract workforce by providing career advice and providing opportunities for staff working on the contract with in-work progression career development into known skills shortages or high growth areas. Illustrative examples: mentoring; mock interviews; CV advice and careers guidance; learning and development; volunteering; influencing staff, suppliers, customers, and communities through the delivery of the contract to support employment and skills opportunities in high growth sectors.

- Support for educational attainment relevant to the contract, including training schemes that address skills gaps and result in recognised qualifications.

For KSL-8 the Supplier shall maintain records of relevant learning interventions and report on the number of hours delivered at the end of each fiscal Quarter.

The Target Performance Level of 140 hours per FTE relates to the initial two-year term of the contract, meaning that the hours reported each Quarter will be accepted as progress towards meeting this target over the life of the contract.

2 Subsidiary Service Levels

2.1 Posting Transactions

Ref.	Subsidiary Service Level	Description	Measure
SSL1-1	Pentip	All Penalty Payment transactions are mapped and submitted to SSCL via journal for upload into Oracle financials	% Completed Daily by 6pm
SSL1-2	Fee Account/PBA	All customer Direct Debit transactions are loaded to the customer account as identified in the data feed	% Completed On day of receipt by 6pm
SSL1-3	MCOL PCOL	All MCOL and PCOL DD transactions will be loaded against the correct customer account	% Completed On day of receipt by 6pm
SSL1-4	Rolls	All Rolls Building online fee transactions are brought to account using the correct mapping and customer accounts	% Completed Daily by 6pm
SSL1-5	Magistrates Expenses	All transactions are loaded against the correct account	% Completed On day of receipt by 6pm
SSL1-6	Magistrates Banking Return	All banking return transactions are mapped and accounted to correct codes	% Completed Daily by 6pm
SSL1-7	BAR/ Portal	All transactions mapped and accounted to correct codes	% Completed Daily by 6pm
SSL1-8	Reform APIs	All transactions mapped and accounted to correct codes	% Completed Daily by 6pm
SSL1-9	General	All SOP uploads are submitted for posting	% Completed Daily by 6pm

Where, for the calculation of the Key Service Level, see section 1.2:

C1 = Number of Penalty Payment transactions mapped to the correct account and submitted to SSCL via journal for upload into Oracle financials, by 6pm.

T1 = Total number of Penalty Payment transactions due to be loaded against the correct customer account and submitted to SSCL by 6pm.

C2 = Number of customer Direct Debit transactions correctly loaded to the customer account as identified in the data feed, on the day of receipt, by 6pm

T2 = Total number of customer Direct Debit transactions due to be brought to account by 6pm

C3 = Number of MCOL and PCOL DD transactions loaded against the correct customer account, by 6pm.
T3 = Total number of MCOL and PCOL DD transactions due to be brought to account by 6pm

C4 = Number of Rolls Building online fee transactions brought to account using the correct mapping and customer accounts, by 6pm.
T4 = Total number of Rolls Building online fee transactions due to be brought to account by 6pm

C5 = Number of Magistrates Expenses transactions are loaded against the correct account, by 6pm.
T5 = Total number of Magistrates Expenses transactions due to be loaded against the correct account by 6pm.

C6 = Number of Magistrates banking return transactions mapped and accounted to correct codes, by 6pm
T6 = Total number of Magistrates banking return transactions due to be mapped and accounted to correct codes by 6pm

C7 = Number of BAR/Portal transactions mapped and accounted to correct codes, by 6pm
T7 = Total number of BAR/Portal transactions due to be mapped and accounted to correct codes by 6pm

C8 = Number of Reform API transactions mapped and accounted to correct codes, by 6pm
T8 = Total number of Reform API transactions due to be mapped and accounted to correct codes by 6pm

C9 = Number of SOP uploads submitted for posting, by 6pm
T9 = Total number of SOP uploads due to be submitted for posting

2.2 Direct Debits

Ref.	Subsidiary Service Level	Description	Measure
SSL2 - 1	General	All monthly DD advance notifications and collections are processed in accordance with customer contracts	% Advance notification sent by 5th of month for collection around 28th of month
SSL2 - 2	General	All weekly DD advance notifications and collections are processed in accordance with customer contracts	% Advance notification issued on Tuesday for collection on Friday of that week
SSL2 - 3	PBA & DD Solutions	AR interfaces are generated and submitted to SSCL ready for upload within one working day of receipt into the Liberata DD System.	% files are completed and sent for loading by 6:00pm
SSL2 – 4	General	All DD collections will be in accordance with the DD mandate	% On day of receipt by 6pm
SSL2 – 5	Credit Limits	All “calls” on customer credit levels are correctly responded to	99% “real time” via API and fee account
SSL2 – 6	Credit Limits	All notifications to customers at 80% of their credit limit are sent	% by 6pm on day that the threshold is reached
SSL2 – 7	Updating accounts	Customer requests for amendments, set up and deletions to be actioned	% Within three WDs of receipt of request
SSL2 – 8	Refunds	All refunds will be actioned in accordance with agreed protocols	% At next agreed advance notification
SSL2 – 9	DD failures	All customer accounts will be placed on hold if credit limit exceeded, DD fails, mandate expired, mandate invalid or upon HMCTS request	% Within 4 hours of notification or instruction

Where, for the calculation of the Key Service Level, see section 1.2:

C1 = Number of monthly DD advance notifications and collections processed in accordance with customer contracts and advanced notification sent out by 5th of the month and collection made around 28th of the month.

T1 = Total number of monthly DD advance notifications and collections due to be processed in accordance with customer contracts and advanced notification sent out by 5th of the month and collection made around 28th of the month.

C2 = Number weekly DD advance notifications and collections processed in accordance with customer contracts and advance notification issued on Tuesday and collection made on Friday of that week.

T2 = Total number of weekly DD advance notifications and collections due to be processed in accordance with customer contracts and advance notification issued on Tuesday and collection made on Friday of that week.

C3 = Number of interface files generated and submitted to SSCL for processing by 6pm.

T3 = Total number of interface files due to be generated and submitted to SSCL for processing by 6pm.

C4 = Number of DD collections completed in accordance with the DD mandate and by 6pm on day of receipt.

T4 = Total number of DD collections due to be completed in accordance with the DD mandate and by 6pm on day of receipt.

C5 = Number of successfully responded to calls on the customer's account to determine credit limit by 6pm.

T5 = Total number of calls on the customer's account to determine the credit limit by 6pm.

C6 = Number of notifications to customers at 80% of their credit limit sent by 6pm on day that the threshold is reached.

T6 = Total number of notifications to customers at 80% of their credit limit due to be sent by 6pm on day that the threshold is reached.

C7 = Number of customer requests for amendments, set up and deletions that have been actioned in the reporting period were actioned within three working days of receipt of request.

T7 = Total number of customer requests for amendments, set up and deletions that have been requested in the reporting period.

C8 = Number of refunds actioned in accordance with agreed protocols, at the next agreed advance notification.

T8 = Total number of refunds due to be actioned in accordance with agreed protocols, at the next agreed advance notification.

C9 = Number of customer accounts placed on hold, where credit limit exceeded, DD fails, mandate expired, mandate invalid or upon HMCTS request, within 4 hours of notification or instruction.

T9 = Total number of customer accounts due to be placed on hold, where credit limit exceeded, DD fails, mandate expired, mandate invalid or upon HMCTS request, within 4 hours of notification or instruction.

2.3 Payments out

Ref.	Subsidiary Service Level	Description	Measure
SSL3-1	Penalty Payments	All refunds are processed within agreed timescales	% Card refunds by 6pm on Friday and cheques/BACS by 6pm on Tuesday
SSL3-2	CAPS	All BACS payments requests are processed and paid to the correct recipient in the next available weekly/ monthly BACS run	% Cheques printed and posted by 6pm. BACS completed by 6pm
SSL3-3	Fee refunds via refund portal	All refunds are made on first available payment file	% Cheques printed and posted by 6pm. BACS completed by 6pm
SSL3-4	Payments and Secure Cheque Printing	All cheque payments are made within one WD after validation	% Cheques printed and posted by 6pm
SSL3-5	Payments and Secure Cheque Printing	All rejected BACS payments are replaced with Cheque payments within one WD of notification	% Cheques printed and posted by 6pm
SSL3-6	BACS	BACS payment requests are processed and submitted to the bank	% BACS completed by 6pm on same day for requests received before 12 noon and next WD for those received after daily cut off
SSL3-7	Mags T&S	Process payment file of approved claims received by agreed cut off date on a weekly basis	% BACS completed by 6pm
SSL3-8	Refunds (MCOL/PCOL and Fee account)	All refunds to be made by agreed protocols	% Card refunds by 6pm and cheques/BACS by 6pm
SSL3-9	Refunds (reformed services)	Validated requests for refunds received by 11am are actioned by 6:00pm on day of receipt (those received later by 6:00pm the following day)	% Card refunds by 6pm and cheques/BACS by 6pm

Where, for the calculation of the Key Service Level, see section 1.2:

C1 = Number of refunds successfully processed in accordance with approved schedule.
T1 = Total number of refunds due to be processed in accordance with approved schedule.

C2 = Number of CAPS payments successfully processed in accordance with approved schedule.
T2 = Total number of CAPS payments due to be processed in accordance with approved schedule.

C3 = Number of refunds successfully processed in accordance with approved schedule.
T3 = Total number of refunds due to be processed in accordance with approved schedule.

C4 = Number of payments and secure cheques successfully made within one WD of validation.
T4 = Total number payments and secure cheques due to be made within one WD of validation.

C5 = Number of rejected BACS payments successfully issued as a cheque within one WD of failure notification.
T5 = Total number of rejected BACS payments due to be issued as a cheque within one WD of failure notification.

C6 = Number of BACS payments successfully processed in accordance with approved schedule.
T6 = Total number of BACS payments due to be processed in accordance with approved schedule.

C7 = Number of approved claims successfully paid in accordance with approved schedule.
T7 = Total number of approved claims due to be paid in accordance with approved schedule.

C8 = Number of refunds successfully processed in accordance with approved schedule.
C8 = Total number of refunds due to be processed in accordance with approved schedule.

C9 = Number of refunds successfully processed in accordance with approved schedule.

T9 = Total number of refunds due to be processed in accordance with approved schedule.

2.4 Account reconciliations

Ref.	Subsidiary Service Level	Description	Measure
SSL4-1	Mags Banking returns/Mags BACS	All reconciliations are completed daily	% Daily (Monday to Friday) by 6pm
SSL4-2	Bail	All reconciliations are completed daily	% On day of receipt by 6pm
SSL4-3	Penalty payments	All reconciliations are completed daily	% On day of receipt by 6pm
SSL4-4	Penalty payments	All un-reconciled items escalated within 5 working days by 6:00pm.	% By 6pm on WD 5
SSL4-5	CAPS	All reconciliations are completed daily	% Daily (Monday to Friday) by 6pm
SSL4-6	BAR/Portal	All reconciliations are completed daily	% Daily (Monday to Friday) by 6pm
SSL4-7	Reformed Services	All reconciliations are completed daily	% Daily (Monday to Friday) by 6pm
SSL4-8	IAC	All reconciliations are completed daily	% Daily (Monday to Friday) by 6pm
SSL4-9	Rolls/ CE file	All reconciliations are completed daily	% Daily (Monday to Friday) by 6pm
SSL4-10	Rolls/ CE file	All un-reconciled items are escalated within 2 WDs	% By 6pm on WD 2
SSL4 -11	Banking Admin and other services	All monthly reconciliations will be completed to agreed timelines	% By 6pm on WD8

Where, for the calculation of the Key Service Level, see section 1.2:

C1 = Number of reconciliations successfully completed by 6pm.

T1 = Total number of reconciliations due to be completed by 6pm.

C2 = Number of reconciliations successfully completed by 6pm.

T2 = Total number of reconciliations due to be completed by 6pm.

C3 = Number of reconciliations successfully completed by 6pm.
T3 = Total number of reconciliations due to be completed by 6pm.

C4 = Number of items successfully escalated by 6pm.
T4 = Total number of items due to be escalated by 6pm.

C5 = Number of reconciliations successfully completed by 6pm.
T5 = Total number of reconciliations due to be completed by 6pm.

C6 = Number of reconciliations successfully completed by 6pm.
T6 = Total number of reconciliations due to be completed by 6pm.

C7 = Number of reconciliations successfully completed by 6pm.
T7 = Total number of reconciliations due to be completed by 6pm.

C8 = Number of reconciliations successfully completed by 6pm.
T8 = Total number of reconciliations due to be completed by 6pm.

C9 = Number of reconciliations successfully completed by 6pm.
T9 = Total number of reconciliations due to be completed by 6pm.

C10 = Number of items successfully escalated by 6pm.
T10 = Total number of items due to be escalated by 6pm.

C11 = Number of reconciliations successfully completed by 6pm.

T11 = Total number of reconciliations due to be completed by 6pm.

2.5 Bank Account management and reconciliations

Ref.	Subsidiary Service Level	Description	Measure
SSL5-1	Roadside deposits	All individual deposits are reconciled to the bank and Pentip on day of receipt	% Daily (Monday to Friday) by 6pm
SSL5-2	Banking	All bank accounts are reconciled daily	% Daily (Monday to Friday) by 6pm
SSL5-3	Banking	All monthly reconciliations are completed and reported on to agreed timelines	% By 6pm on WD8
SSL5-4	Bail	All virtual accounts and reconciled to the GL and tracker	% Daily (Monday to Friday) by 6pm
SSL5-5	Sweeps	All sweeps are calculated and completed and reconciled in accordance with agreed timelines	% Daily (Monday to Friday) by 6pm for the reconciliation % Daily (Monday to Friday) per bank deadline for the sweeps
SSL5-6	Bank transfers	All transfers are completed in accordance with agreed timelines	% Daily (Monday to Friday) per GBS/ Commercial bank deadlines

Where, for the calculation of the Key Service Level, see section 1.2:

C1 = Number of reconciliations successfully completed by 6pm.

T1 = Total number of reconciliations due to be completed by 6pm.

C2 = Number of reconciliations successfully completed by 6pm.

T2 = Total number of reconciliations due to be completed by 6pm.

C3 = Number of reconciliations successfully completed by 6pm.

T3 = Total number of reconciliations due to be completed by 6pm.

C4 = Number of reconciliations successfully completed by 6pm.

T4 = Total number of reconciliations due to be completed by 6pm.

C5 = Number of sweeps successfully completed by 6pm.

T5 = Total number of sweeps due to be completed by 6pm.

C6 = Number of transfers successfully completed to agreed schedules.

T6 = Total number of transfers due to be completed to agreed schedules.

2.6 Customer account applications

Ref.	Subsidiary Service Level	Description	Measure
SSL6-1	Fee account / PbA	All customer applications to be processed within 3 WDs of receipt	% By 6pm on 3rd WD after receipt
SSL6-2	MCOL/PCOL	All applications to be processed within 3 WDs of receipt of approved application (comprising authorised application from HMCTS and signed mandate from customer)	% By 6pm on 3rd WD after receipt
SSL6-3	Fee Account/PBA/MCOL/PCOL	Applications requiring further information in support/additional HMCTS approval to be referred to HMCTS within 1 day of initial processing	% By 6pm on 1st WD after initial processing
SSL6-4	Fee Account/PBA/MCOL/PCOL	All customer amendments, set-up and deletion will be actioned within three WDs of receipt of amendment details/paperwork	% By 6pm on 3rd WD after receipt
SSL6-5	Mags T&S	All new accounts created and welcome notification sent to Magistrate	% By 6pm on 3rd WD after receipt
SSL6-6	CE file	All customer applications to be processed within 3 WDs of receipt	% Daily (Monday to Friday) by 6pm on 3rd WD after receipt

Where, for the calculation of the Key Service Level, see section 1.2:

C1 = Number of customer applications successfully processed within 3WD of receipts.

T1 = Total number of customer applications due to be processed within 3WD of receipt.

C2 = Number of customer applications successfully processed within 3WD of receipts.

T2 = Total number of customer applications due to be processed within 3WD of receipt.

C3 = Number of customer applications requiring additional information successfully referred to HMCTS within 1WD of initial processing.

T3 = Total number of customer applications requiring additional information due to be referred to HMCTS within 1WD of initial processing.

C4 = Number of customer accounts created, and notifications sent successfully processed within 3WD of receipt.

T4 = Total number of customer accounts created, and notifications sent due to be processed within 3WD of receipt.

C5 = Number of customer amendments successfully processed within 3WD of receipts.

T5 = Total number of customer amendments due to be processed within 3WD of receipt.

C6 = Number of customer applications successfully processed within 3WD of receipts.

T6 = Total number of customer applications due to be processed within 3WD of receipt.

2.7 Service Availability

Ref.	Subsidiary Service Level	Description	Measure
SSL7-1	Service Availability	Service Availability of all services, during their relevant Service Hours.	% time services are available

Where Service Availability is calculated as below:

2.7.1 Service Availability shall be measured as a percentage of the total time of Extended Service Hours in a Service Period, in accordance with the following formula:

Service Availability % = $\frac{(MP-SD) \times 100}{MP}$

where:

MP = total number of minutes, excluding Permitted Maintenance, of Extended Service Hours within the relevant Service Period; and

SD = total number of minutes of Service Downtime, excluding Permitted Maintenance in the relevant Service Period.

2.7.2 When calculating Service Availability in accordance with this Paragraph 2.7.1:

(i) Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with Clause 2.6 (System Requirements) of the Specification, shall be subtracted from the total number of hours in the relevant Service Period; and

(ii) Service Points shall accrue if any such Service Downtime occurs as a result of:

- Emergency Maintenance undertaken by the Supplier; or
- Permitted Maintenance undertaken by the Supplier that exceeds the agreed period of the permitted maintenance.

3 Key Performance Indicators

3.1 Transactions Loaded into SOP

Ref.	Business Area	Description	Measure	KPI Target
KPI1-1	All services	All entries from validated accounts are brought fully to account by generation and submission of journals to SSCL for upload onto SOP.	By 6pm within one WD of receipt	98%
KPI1-2	All services	All entries from validated accounts are brought fully to account by generation and submission of AR invoice and receipts interfaces to SSCL for upload onto SOP.	By 6pm within one WD of receipt	98%

Where, for the calculation of the Key Performance Level 1:

C1 = Number of journals mapped to the correct account and submitted to SSCL for upload, by 6pm.

T1 = Total number of journals due to be mapped to the correct account and submitted to SSCL for upload, by 6pm.

C2 = Number of AR invoice and receipt interface files mapped to the correct account and submitted to SSCL for upload, by 6pm.

T2 = Total number of AR invoice and receipt interface files due to be mapped to the correct account and submitted to SSCL for upload, by 6pm.

3.2 Management information

Ref.	Business Area	Description	Measure	KPI Target
KPI2-1	All Services	All reports will be delivered in accordance with the requirements as documented in the Liberata Schedule of Reports to agreed timelines	By 6pm on WD8	98%
KPI2-2	All services	All monthly reports, with ability to self-serve, are issued by 5pm on WD 8	By 5pm on WD8	98%

KPI2-3	All services	Provide a MI portal for all data transactions and reports to be stored. All data to be uploaded to agreed timelines	All reports and data to be available by WD8	98%
KPI2-4	All civil fee taking services	Provide monthly reports for fee and remissions for each of the services detailed below detailing volume and value of transactions by fee type	All reports and data to be available by WD8	98%

Where, for the calculation of the Key Performance Level 2:

C1 = Number of reports issued by 6pm on WD8.

T1 = Total number of reports due to be issued by 6pm on WD8.

C2 = Number of reports issued by 5pm on WD8.

T2 = Total number of reports due to be issued by 5pm on WD8.

C3 = Number of data entries uploaded to agreed timelines.

T3 = Total number of data entries due to be uploaded by agreed timelines.

C4 = Number of reports issued by 6pm on WD8.

T4 = Total number of reports due to be issued by 6pm on WD8.

3.3 Cash/Treasury management

Ref.	Business Area	Description	Measure	KPI Target
KPI3-1	Inter-departmental transfers	All calculations and transfers to be completed to agreed timelines	By 6pm on WD8	98%
KPI3-2	Cash transfer	All authorised requests received by 10am to be completed on day of receipt of authorisation	By 6pm on day of receipt of authorisation	98%

KPI3-3	Cash transfer	All authorised requests received after 10am to be completed on next WD after receipt of authorisation	By 6pm on next WD following receipt of authorisation	98%
KPI3-4	Cash Management	Successful sweep of the Commercial accounts to/from the main HMCTS GBS Account to agreed timelines	By 6pm daily	98%
KPI3-5	Cash Management	All accounting entries to be submitted to SSCL for upload and all transfers for the HMCTS third party monies to be completed correctly by 4:00pm on last WD of the month.	By 6pm on last WD	98%
KPI3-6	Magistrates BACS processes	All bank transfers required to support the BACS payment process are completed on the day that payment is debited by 6pm	By 6pm on day amount is debited	98%
KPI3-7	CFER/ MoJ / Home Office Payover	All bank transfers are accounted for and completed within timeline agreed with Trust Statement team	For MoJ Transfer:- by 6pm within 1 WD of notification of the amount to be transferred For Home Office transfer – By 6pm on scheduled dates in the year	100%
KPI3-8	Magistrates domestic and foreign payments	All bank transfers are completed to agreed timelines	By 6pm on 2nd WD after receipt of request.	95%

Where, for the calculation of the Key Performance Level 3:

C1 = Number of transfers completed by 6pm.

T1 = Total number of transfers due to be completed by 6pm.

C2 = Number of transfers completed by 6pm.

T2 = Total number of transfers due to be completed by 6pm.

C3 = Number of transfers completed by 6pm.

T3 = Total number of transfers due to be completed by 6pm.

C4 = Number of sweeps completed by 6pm.

T4 = Total number of sweeps due to be completed by 6pm.

C5 = Number of accounting entries and transfers completed by 6pm.

T5 = Total number of accounting entries and transfers due to be completed by 6pm

C6 = Number of transfers completed by 6pm.

T6 = Total number of transfers due to be completed by 6pm.

C7 = Number of transfers completed by 6pm

T7 = Total number of transfers due to be completed by 6pm.

C8 = Number of transfers completed by 6pm

T8 = Total number of transfers due to be completed by 6pm.

3.4 Deposit Management

Ref.	Business Area	Description	Measure	KPI Target
KPI4-1	Bail	All bail notifications received before 1pm are actioned on the same day (to include deposit creation, release and forfeiture).	Daily by 6pm	98%
KPI4-2	Bail	All bail notifications received after 1pm are actioned on the next WD (to include deposit creation, release and forfeiture).	Daily by 6pm on 1WD after notification	98%
KPI4-3	Bail	All reconciliations and the tracker are updated and completed on each WD by 6pm	Daily by 6pm	98%
KPI4-4	Roadside Deposits	All Pentip notifications relating to roadside deposits are actioned within one day of receipt by 6pm.	Daily by 6pm	98%
KPI4-5	Roadside Deposits	All individual deposits are reconciled to the bank account and Pentip system and the tracker is updated on day of receipt	Daily by 6pm	98%
KPI4-6	Roadside Deposits	All escalations are issued daily and all unpaid deposits are notified to HMCTS on day of identification	Daily by 6pm	98%

KPI4-7	ET deposits	All ET deposit notifications received before 1pm are actioned by 4.30pm on the same day (to include deposit creation, release and forfeiture).	Daily by 6pm	98%
KPI4-8	IAC deposits	All IAC notifications received before 1pm are actioned by 4.30pm on the same day (to include deposit creation, release and forfeiture).	Daily by 6pm	95%

Where, for the calculation of the Key Performance Level 4:

C1 = Number of bail notifications actioned by 6pm.

T1 = Total number of bail notifications due to be actioned by 6pm.

C2 = Number of bail notifications actioned by 6pm.

T2 = Total number of bail notifications due to be actioned by 6pm.

C3 = Number of reconciliations completed by 6pm.

T3 = Total number of reconciliations due to be completed by 6pm.

C4 = Number of notifications actioned by 6pm.

T4 = Total number of notifications due to be actioned by 6pm.

C5 = Number of reconciliations completed by 6pm.

T5 = Total number of reconciliations due to be completed by 6pm.

C6 = Number of escalations completed by 6pm.

T6 = Total number of escalations due to be completed by 6pm.

C7 = Number of notifications actioned by 6pm.

T7 = Total number of notifications due to be actioned by 6pm.

C8 = Number of notifications actioned by 6pm.

T8 = Total number of notifications due to be actioned by 6pm.

3.5 Chargebacks

Ref.	Business Area	Description	Measure	KPI Target
KPI5-1	Chargebacks	All chargebacks are accounted for against the correct bank and business entity within 2 workings days of receipt via submission of an approved GL journal to SSCL to agreed timelines	Daily by 6pm	98%

Where, for the calculation of the Key Performance Level 5:

C1 = Number of chargebacks accounted for within 2 WD by 6pm.

T1 = Total number of chargebacks due to be accounted for within 2 WD by 6pm.

3.6 Helpdesk

Ref.	Business Area	Description	Measure	KPI Target
KPI6-1	Telephone calls	All helpdesk call to be answered within agreed timelines	Calls to be answered within one minute	98%
KPI6-2	Emails	All emails to be acknowledged within agreed timelines	Emails to be acknowledged within 30 minutes	98%
KPI6-3	Queries	All queries to be responded to within agreed timelines	Responses to be within 2 WDs	95%
KPI6-4	Queries	All queries requiring escalation to HMCTS to be escalated within agreed timescales	All queries to be escalated within 3 WDs	98%
KPI6-5	Additional information	All additional information received in respect of a query to be actioned within agreed timelines	Actioned within 3 WD of receipt	98%

Where, for the calculation of the Key Performance Level 6:

C1 = Number of calls answered within one minute.

T1 = Total number of calls due to be answered withing one minute.

C2 = Number of emails acknowledged within 30 minutes.

T2 = Total number of emails due to be acknowledged within 30 minutes.

C3 = Number of responses made within 2WD.

T3 = Total number of responses due to be made within 2WD.

C4 = Number of escalations made within 3WD.

T4 = Total number of escalations due to be made within 3WD.

C4 = Number of actions made within 3WD.

T4 = Total number of actions due to be made within 3WD.

1ANNEX C

GLOSSARY

Glossary and interpretations	**In this Call-Off Contract the following expressions mean:**
Account Code/NAC	10 digit code given to each category used by HMCTS to classify and distinguish financial assets, liabilities, and transactions.
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
API	Application Programming Interface - a software interface which allows two applications to talk to each other.
ARIA	Asylum & Immigration Tribunal fee and case management system
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.
BAR	Banking & Accounting Return - means used by Courts/Tribunals to inform supplier of all daily accounting
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.

Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
CaseMan	County Court case management system
CFER	Consolidated Fund Extra Receipt - Receipts which cannot be used to support expenditure of a Department. Instead they are recorded and passed to the Treasury's Consolidated Fund. These include taxes collected by Departments.
Chargeback	A transaction reversal made to dispute a card transaction
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
CMC	Civil Money Claims - digitalised service for issuing money claims
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.
Commercial Contract Manager	This is the MOJ Commercial Contract Manager representing MOJ/HMCTS.
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').
Consolidated fund	The central account administered by HM Treasury which receives government revenues and makes issues to fund expenditure by Government Departments.

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 Data Protection Legislation.
Cost Centre	8 digit code given to a segment of HMCTS for which costs are required to be collected and formally reported on separately
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	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing by the Processor under this Call-Off Contract on the protection of Personal Data.
Data Protection Legislation	Data Protection Legislation means: i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; iii) all applicable Law about the processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.
Data Subject	Takes the meaning given in the Data Protection Legislation.
DCN	Document control number. This is a unique reference assigned to scanned documents by the bulk scanning provider
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract. Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework

	Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
[REDACTED]	[REDACTED]
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.
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
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Fee Account/PBA/Payment by Account	Service allowing approved customers to transact with HMCTS online, by post or in person, by quoting their unique reference. Payment made by weekly/monthly direct debit

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 Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FOIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.
GBS	Government Banking Service

G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679).
GL	General Ledger
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.
Gov.UK Pay	A free service, available to public sector organisations to take online card payments. There's no monthly charge, no set-up fee and no procurement process. It enables service teams to replace offline payment methods quickly and easily, providing a Payment Card Industry (PCI) fully compliant, secure and accessible user experience hosted on GOV.UK.
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.
HMT	Her Majesty's Treasury
IAC	Immigration & Asylum Chamber
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 Section 2
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).
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.
KPI	Key Performance Indicators
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.
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 Framework ITT and Lots will be construed accordingly.

Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers, (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6, (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
MBR	Magistrates Banking Return process used by accounting units to notify supplier of fine income receipts and payments to be made
MCOL	Money Claims Online - system enabling customers to commence debt recovery action and pay by debit/credit card or weekly/monthly direct debit
Memo lines	Predefined lines that can be selected from a list of values when raising invoices and credit/debit memos.
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.
MyHMCTS	Online case management system for legal professionals allowing them to submit and pay for online applications for probate, divorce, financial remedy, family public law orders and immigration and asylum cases
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.

Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
PCI-DSS	Payment Card Industry Data Security Standards
PCOL	Possession Claims Online - system enabling customers to commence possession action online for non-payment of rent or mortgage and pay by debit/credit card or weekly/monthly direct debit
Pentip	The system used to administer fixed penalty notices and Public notices of Disorder.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.

Protective Measures	Appropriate technical and organisational measures which may include: 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 Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Service Data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service Definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service Description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Services	The services ordered by the Buyer as set out in the Order Form.
SLA	Service Level Agreements

SOP	The Single Operating Platform, a set of integrated computer programmes that share a common underlying database structure. The SOP solution is largely based on the latest version of Oracle's E-Business Suite (EBS)
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
SSCL	Shared Services Connected Limited, a joint venture between Steria and Cabinet Office. SSCL deliver financial and procurement services for the MoJ (including HMCTS).
Start Date	The start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a Subcontract, (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier Staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
TEC	Traffic Enforcement Centre
Term	The term of this Call-Off Contract as set out in the Order Form.
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Annex D

Changes Requests and Variations

Contents

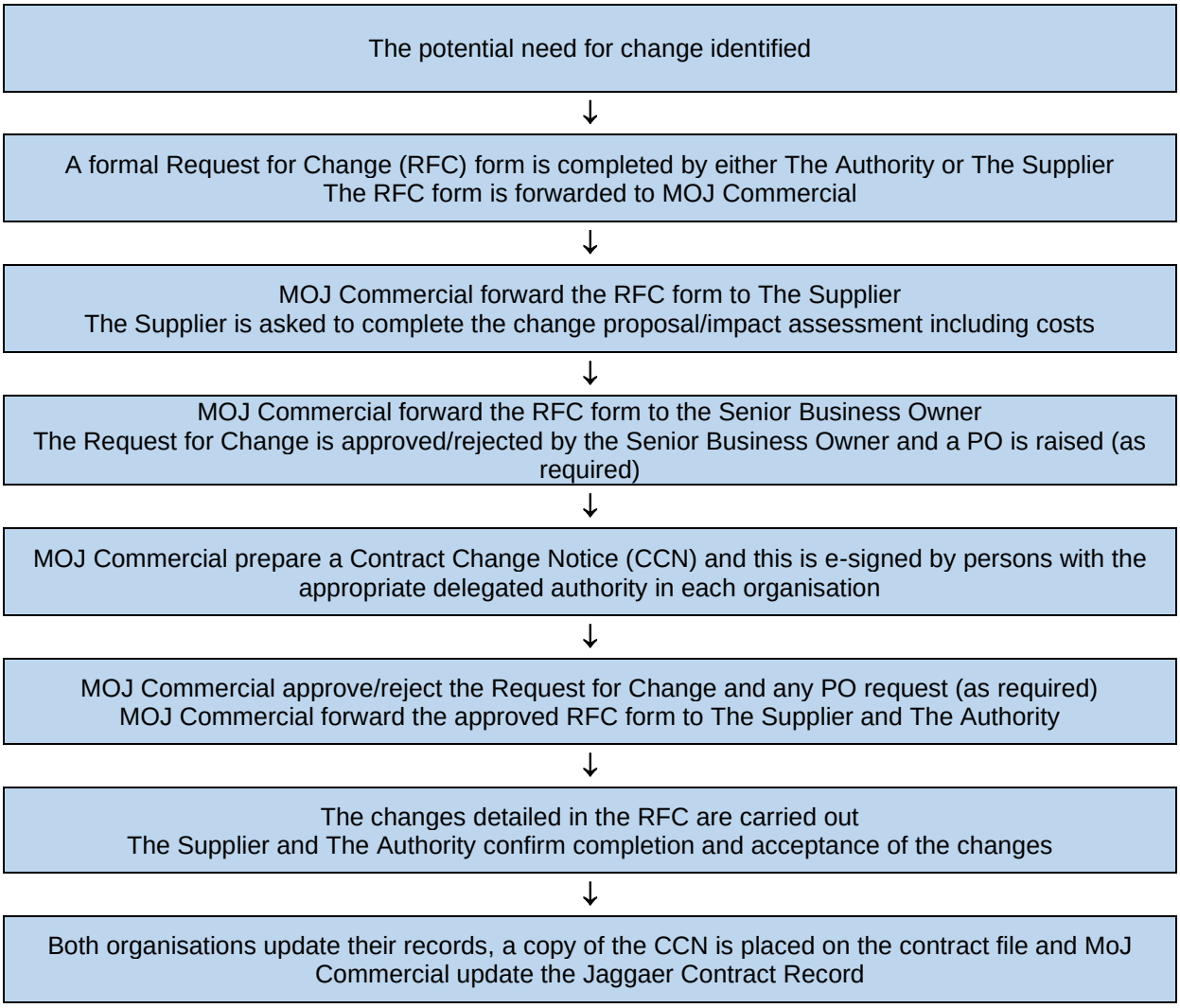
1.1. Who can request a change?

A change may be requested by HMCTS, MOJ Commercial or by Liberata.

1.2. The Request for Change and Variation process

A contract variation may be implemented when a change is required to a contract where consideration will be exchanged. Consideration could be in the form of changing the range of services, the number of goods, the pricing mechanism, or the duration of the contract.

The flowchart below outlines the steps to be followed as part of the Request for Change and Variation process.



1.3. Request for Change Form Template

Request for Change

Contract Title	Con_xxxx Financial Transaction Processing
Name of Supplier	Liberata UK Ltd
RFC Number (allocated by MOJ Commercial)	
PART 1 – Details of Change Request (to be completed by Business Service Owners only)	
Description of change to service required:	
Reason for change:	
Change Requested by (name)	
Email	
Signature	
Date	
Approval to Request RFC (name)	
Email	
Signature	
Date	
Please pass this form to MOJ Commercial – CCMDOpenJusice@justice.gov.uk **THIS FORM SHOULD ONLY BE SUBMITTED TO MOJ COMMERCIAL**	
PART 2 – Impact Analysis by Supplier (to be completed by Liberata)	
Proposal:	

Assumptions:
Dependencies:
Cost of Change – indicate whether Fixed/Variable costs or T&M costs:

PART 3 – Decision (to be completed by Senior Business Owner)		
AUTHORISED	☐	Reason for refusal/deferral:
REFUSED	☐	
DEFERRED	☐	Deferred date:

Decision Confirmed by (name)	
Email	
Signature	
Date	

PART 4 – Approval (to be completed by MOJ Commercial)		
APPROVED	☐	PO Number & Value:
REFUSED	☐	Reason for refusal/deferral:
DEFERRED	☐	Deferred date:

Approval Confirmed by (name)	
Email	
Signature	
Date	

PART 5 – Date Completed (To be completed by Liberata)	
Actioned as per quotation?	Y / N
Date Closed	
Any Comments?	
Confirmed by (name)	
Email	
Date	
PART 6 - User Acceptance	
User Acceptance Confirmed by (name)	
Email	
Date	

1.4. Contract Change Notice (CCN) Template

For completion by the Authority once the Change has been agreed in principle by both Parties. Changes do not become effective until this form has been signed by both Parties.

Contract Change Notice (CCN)

Contract Title: Con_xxxx Financial Transaction Processing	**Change requested by:**
Name of Supplier: Liberata UK Ltd	
Change Number:	
Date on which Change takes effect:	
Contract between: The Secretary of State for Justice and Liberata UK Ltd	
It is agreed that the Contract is amended, in accordance with Regulation 72 of the Public Contracts Regulations 2015, as follows: **Where significant changes have been made to the Contract, information previously published on Contracts Finder will be updated.**	
Words and expressions in this CCN shall have the meanings given to them in the Contract. The Contract, including any previous CCNs, shall remain effective and unaltered except as amended by this CCN	

Signed for and on behalf of the Secretary of State for Justice		**Signed for and on behalf of Liberata UK Ltd**	
Signature		**Signature**	
Name		**Name**	
Title		**Title**	
Date		**Date**	

SECURITY ASPECTS LETTER

Liberata UK Limited

For the attention of [REDACTED] Date: 24/08/2022

Dear [REDACTED]

SUBJECT: Security Aspects Letter - HMCTS

TENDER NO: [REDACTED]

1. The above tender arises from a United Kingdom government contract and will involve your company holding UK classified material. It is a condition of this tender that this material must be protected. The standard of protection required has been notified to you separately and varies with the level of classification. Material passed to you will bear the classification appropriate to it. However, to assist you in allocating any necessary classification to material which your company may produce during the course of the tender and thus enable you to provide the appropriate degree of protection to it, this letter formally advises you of the correct classification to apply to the various aspects of the tender.

2. The aspects of the tender which require to be classified are:

ASPECTS	CLASSIFICATION
Security Architecture	OFFICIAL
Detail of Security Enforcing Functions	OFFICIAL
Security Vulnerabilities	OFFICIAL
Risks to Data, Applications and Infrastructure	OFFICIAL
Source Code/Memory Dumps	OFFICIAL
Security Incident Reports	OFFICIAL
Sensitive Personal Data	OFFICIAL Sensitive
Network Diagrams	OFFICIAL
Aggregated Data (as advised by the Authority)	OFFICIAL
Configuration data	OFFICIAL
Credentials for Live Services	OFFICIAL
Cryptographic Design and Procedures	OFFICIAL
All Other Aspects	OFFICIAL

3. It is essential that any sub-contractor with the potential to produce material which may be classified OFFICIAL SENSITIVE is provided with a SAL from you. Any such sub-contractor SAL must be agreed by the Authority before issue.

4. You are requested to acknowledge receipt of this letter and to confirm that the level of classification associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this tender that they are fully understood, and that the required security controls in the contract security conditions can and will be taken to safeguard the material concerned.

5. If you have any difficulty in interpreting the meaning of the above aspects or in safeguarding the materials, will you please let me know immediately.

- End -