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	281143385400349
Call-Off Contract reference	Con_18914
Call-Off Contract title	Legal Case Management system for the OSPT
Call-Off Contract description	Official Solicitor & Public Trustee Case (OSPT) Management System
Start date	23/04/2021
Expiry date	22/04/2023
Call-Off Contract value	£299,500.00
Charging method	BACS
Purchase order number	To be confirmed upon contract signature.

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	The Secretary of State for Justice on behalf of the Ministry of Justice The Ministry of Justice 102 Petty France Westminster London SW1H 9AJ
To the Supplier	Civica Uk Ltd South Bank Central 30 Stamford Street London SE1 9LQ United Kingdom Company number: 01628868
Together the 'Parties'	

Principal contact details

For the Buyer:

Operations:

Title: Portfolio Manager

[REDACTED]

Commercial Contact:
Title: Commercial Manager
[REDACTED]

For the Supplier:

Account Manager

[REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **23/04/201** 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). For the avoidance of doubt should the buyer terminate the contract under clause 18.1 then the Charges for the Annual SaaS fee for the current contract year will remain payable.
Extension period	This Call-off Contract can be extended by the Buyer for **two** period(s) of 12 months each, by giving the Supplier **four weeks** 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	Civica Case Management (iCasework) for up to 150 users. [REDACTED]
Additional Services	[REDACTED]
Location	Remote working. Should Covid-19 restrictions lift the Services may be delivered to: [REDACTED]
Quality standards	The quality standards for this Call-Off contract are: As specified in the Supplier's G-Cloud Offers. See section 14 of this contract.
Technical standards:	The technical standards required for this Call-Off Contract are: • in accordance with the requirements of the G-Cloud 12Framework • including adherence to the Technology Code of Practice.

Service level agreement:	The service level and availability criteria required for this Call-Off Contract are **detailed in appendix one**
Onboarding	A high level on boarding plan is included in Appendix Two. The parties will agree and sign off a detailed implementation plan including acceptance criteria for UAT and other project and payment milestones including support service integration and procedures within 30 days of contract signature
Offboarding	The offboarding plan for this Call-Off Contract is detailed in the Service level agreement in appendix one
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 [**£374,375** 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 **£374,375** 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 ● professional indemnity insurance 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 limit the Buyer requires (and as required by Law) employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 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. Clauses 7.4 to 7.13 of the Framework Agreement. 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

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

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, Government Internal Audit Agency, the Comptroller 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

11

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

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**:** The Buyer is responsible for providing access to the Supplier to data for the purpose of data conversion, the licensing of MS Office and other associated desktop application software, Internet connectivity from the Buyer's premises and provision of a contemporary Internet browser on each user's device to allow access to the Supplier's service. Specifically, the Buyer is responsible for 1. Coordination with CGI for the uploading of data to the migration platform in ljne with project timelines, for test and live migrations.Data to be supplied being the Prescient+ SQL database, and the associated document store. The parties agree that they will agree an alternative method of data load should the primary method be unavailable. 2. Technical coordination in ljne with project timelines of access to the iCasework platform including email and Single sign on (where required) 3. Timely availability of resources to provide input into the customisation program, and UAT testing.
Buyer's equipment	The Buyer is responsible for, the licensing of MS Office and other associated desktop application software, Internet connectivity from the Buyer's premises and provision of a contemporary Internet browser on each users device to allow access to the Supplier's service.

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 BACS.
Payment profile	The payment profile for this call off contract is 1. SaaS service, payable annually in advance. The first year payment will be £82,500 (Representing 11/12th of the annual fee of £90,000)payable 30 days after contract signature The Second year the SaaS service will be payable on the first anniversary of the agreement for a full 12 months £90,000 [REDACTED] For the avoidance of doubt should the buyer terminate the contract under clause 18.1 then there will be no refund of any annual SaaS fee paid in advance.
Invoice details	The Supplier will issue electronic invoices monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Invoices will be sent to: [REDACTED] Post: Ministry of Justice Finance & Accounting Shared Services Connected Limited PO Box 766 Newport, Gwent NP20 9BB [REDACTED]

Invoice information required	All invoices must include the purchase order and contract number.
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	The total value of this Call-Off Contract is £299,500
Call-Off Contract charges	[REDACTED]

Additional Buyer terms

Performance of the Service and Deliverables	This Call-Off Contract will include the following, Implementation Plan, exit and offboarding plans and milestones: Implementation plan as detailed in Appendix Two, and as further agreed. Off boarding as detailed in Service Level Agreement in Appendix One
Guarantee	N/A
Warranties, representations	N/A

Supplemental requirements in addition to the Call-Off terms	N/A
Alternative clauses	N/A
Buyer specific amendments to/refinements of the Call-Off Contract terms	N/A
Public Services Network (PSN)	N/A
Personal Data and Data Subjects	Annex 1

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	Supplier	Buyer
Name	[REDACTED]	[REDACTED]
Title	[REDACTED]	[REDACTED]
Signature	[REDACTED]	[REDACTED]
Date	[REDACTED]	[REDACTED]

Schedule 1: Services

[REDACTED]

[REDACTED]

Schedule 2: Call-Off Contract charges

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]

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. (see https://www.digitalmarketplace.service.gov.uk/g-cloud/services/281143385400349).

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 The Supplier will ensure that:

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

9.2.2 the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

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

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

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

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

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

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

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

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

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

9.7 The Supplier will notify 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.

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

9.8.1 premiums, which it will pay promptly
9.8.2 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 15 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'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- 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 in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the 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 additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

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

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls

process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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 additional exit plan.

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

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

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

N/A

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

N/A

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, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the 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:
	• 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: 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: There are 28 items of personal data that could be held and these are identified on the DPIA in section 1.7 .
Duration of the Processing	The duration of the processing will be for the length of the contract
Nature and purposes of the Processing	The Buyer will be processing data under the GDPR and Part 3 of the Data Protection Act 2018. GDPR allows the processing of personal data if it is necessary for the performance of a task carried out in the public interest. The buyer is tasked with the administration of justice which

	includes providing everyone with legal representation.
Type of Personal Data	The following items are available to be viewed 1. Title 2. Surname 3. Forenames 4. Date of Birth 5. Sex 6. Alias forenames & surnames 7. National Insurance number 8. Address including postcode 9. Home telephone number 10. Business telephone number - solicitors may not be clients, about 90% is with solicitors, but occasions for client details and their capability 11. Mobile telephone number 12. Email addresses - very few clients email - its to do with capacity 13. Driving licence, passport or birth certificate pdf copies for ID 14. Warning markings (to perform risk assessment) - yes/no answer about their behaviour ▪ are they threat 15. Protective markings 16. Date of hearing 17. Mainly civil work, so parties would be listed as court reference title - do have international child abduction, so may refer to criminal sometimes minimal 18. Notes

	19. Some civil cases involving prisoners - again PDF and correspondence about the prisoner - so release dates, length of sentence and date of sentence and crime - background info for us - bail 20. Court venue 21. Custody Details - would have the details of the court directions after the hearing - recovery/release of child 22. Photos of missing children and parents 23. Wanted/Missing Reports - with the child abduction pdf's 24. Arrest/Summons History - ancedotal 25. Impending Prosecutions - linked to prisoner pdf 26. Occupations 27. Address History (i.e. not just Address including postcode as per your list) - just for case life if they move during its lifetime 28. Secondary address (possible overseas)
Categories of Data Subject	The following categories of data subject may exist • clients • suppliers • staff/former staff • temporary workers • persons contracted to provide a service • claimants • volunteers • agents • service users • complainants, enquirers or their representatives • professional advisers and consultants • carers, representatives or legal guardians • landlords • witnesses • offenders and suspected offenders • licence and permit holders • traders and others subject to inspection • people captured by CCTV images • representatives of other organisations • members of the public
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	In the event the Supplier is no longer the contractor at the end of the contract term, all data will be returned to the Buyer in advance of the end of the contract in line with the Exit Plan. Once the data has been returned the Supplier

	will take all necessary steps to ensure they hold no copy of the data that has been received from the Buyer after the end of the contract, this includes backup and archive materials..

Annex 2: Joint Controller Agreement N/A

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 4 of the Framework Agreement (Where one Party is Controller and the other Party is Processor) and paragraphs 17-27 of Schedule 4 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [**delete as appropriate Supplier/Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**Supplier's/Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a data subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every **[enter number]** months on:

(i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses

2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

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

(i) are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or

divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;

and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant central government body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant central government body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial

Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clauses 8.66 to 8.79 of the Framework terms (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Not used

9. Termination

9.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (joint controller agreement), the Buyer shall be entitled to terminate the contract by issuing a termination notice to the Supplier in accordance with Clause 18.5 (Ending the contract).

10. Sub-Processing

10.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

11. Data Retention

11.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

iCasework for Legal

Support Service Description and Service Level Agreement

Contents

Support Service Description

Our preferred method of contact for support issues is via our support portal; the support team may also be contacted via telephone and email.

This document describes our support model, detailing the support services, support resources, contact information and best practices for contacting our support team.

Definition of support

After your system has gone "Live", we provide all clients with ongoing technical support. Our support team manages system issues, queries, service and change requests as well as training requirements. The team also processes software releases, updates and patches for bugs including security updates. Support is provided through named, nominated users (**System administrators**) whose details have been provided by the client in the development stages of the project.

At Civica we have three priority levels relating to system issues:

Priority	Definition
Critical (1)	An issue which may result in the complete loss of the iCasework system (system down).
Impaired (2)	An issue that affects many users and disrupts the normal running of the system.
Minimal (3)	An issue that has minimal impact and does not affect the normal running of the system or for which a workaround is available.

What is the definition of an issue?

A problem that affects the normal running of the system.

What is the definition of a query?

A query is a question about the functionality or operation of the system.

What is the definition of a change?

A change is an alteration to the functionality or operation of the system.

What are the responsibilities of the System administrator?

This is person responsible for making sure the system runs smoothly within the business. This includes user management, report and follow-up of issues via the support portal, correspondence templates, branding, service menu, classifications, etc.

How to contact iCasework's support team

Our support team aims to resolve all enquiries at first point of contact and in the shortest possible time. All issues must be reported to us in English and responses to issues will also be sent to clients in English. We would prefer that all enquiries are logged via the support portal as this is accessible 24 hours a day, seven days a week. The support team can be reached by phone in the UK on **Monday to Friday, 9am to 5.30pm** (excluding UK Bank and Public Holidays). There are three channels to contact the support team for iCasework applications:

[REDACTED]

The iCasework support portal requires a username and password to access the system. The credentials to access the support portal are provided to the **Client Nominated Contact** just before the client's system "Go Live" when the system is handed over from the project team to the support team. Civica expects that all clients will manage these access details in a secure manner.

Reporting an issue

Before any issue is reported to the support team, it is imperative that the issue has been replicated by the system administrator so we know the problem is not internal or localised to the user. The **System administrator** will be required to provide the following information when contacting support:

- Name, organisation, email address and telephone number
- Ticket number (if the client has their own ticketing system)
- The name of the service affected
- The type of request (problem, question, services or training request, etc.)
- A detailed description of the problem (include screenshots if possible)
- How many users are affected (one or many)
- What were the affected user(s) doing that led to the problem manifesting itself (if known)
- Were there any recent changes in the local infrastructure (for example, browser version)
- Examples/errors, case numbers and screenshots of the problem when tested by the **System administrator**

Clients will be required to ensure that at least one member of the team (although ideally more than one) has been trained at an administrator level and this person is aware of the features and responsibilities of this role.

Our Support team is available to assist with all technical issues of varying degrees of priority. However, please have in mind that in order to resolve issues efficiently and effectively, Civica needs to be able to reproduce the issue the client is experiencing. We ask that our clients provide us with as much detail as possible, so we can attempt to reproduce the error within our environment or where needed, Clients provide permission for Civica to access the Customer system to view the error. Where required relevant diagnostic tools will be deployed on the platform to support diagnosis for intermittent issues.

Timescales

The following table outlines the response time objectives that Civica aims to achieve when a client submits a support request. Measurements are from the time Civica receives the initial request for support, to the time Civica provides an initial communication back to the client regarding the request.

Priority	Definition	Initial response time objective	Response time coverage
1	**Critical:** Business critical functionality is inoperable or critical interface has failed. This applies to a production environment and indicates an inability to access	Acknowledgement within 30 minutes of the fault being raised. Resolution	hours a day, 7 days a week (24x7)

What can you expect from iCasework support?

	services resulting in a critical impact on operations. This condition requires an immediate solution.	within 2 hours of acknowledgement	
2	**Impaired (significant business impact):** A service business feature or function of the service is severely restricted in its use.	Acknowledgement within 60 minutes of the fault being raised. Resolution within 8 Working Hours of acknowledgement	Monday to Friday 9am to 5:30pm (GMT/BST), excluding Bank and Public Holidays ("Working Hours")

3	**Minimal (minor business impact):** Indicates an issue with the service or functionality which is not causing a critical impact or severe restriction on operations or for which a workaround is available.	Acknowledgement within 8 Working Hours of the fault being raised. Resolution within 5 working days of acknowledgement.	Monday to Friday 9am to 5:30pm (GMT/BST), excluding Bank and Public Holidays

Escalations

If clients are not happy with the way an enquiry has been dealt with, they can escalate the case to the Support Manager, so a more in-depth investigation can take place. If the Support Manager is not able to resolve the case then the issue will be escalated to the Product Manager for final consideration. All information about the case will be available via the support portal and the team will add regular updates to the system to keep clients informed at every stage of the investigation.

Knowledge management

Answers for most frequent client questions can be found in our extensive information pages (wiki) covering our entire solution. The wiki contains FAQs, how-to guides as well as a wide range of training videos.

We strongly suggest that clients check the wiki and the iCasework YouTube channel before logging an issue.

The wiki is available at: https://icasework.atlassian.net/wiki/display/UsefulFeedback and our YouTube channel at: https://www.youtube.com/user/iCasework

Queries

Queries about general usage of the system may be logged via the standard contact mechanisms associated with Support. General queries are not allocated a specific response time, but are referred to and addressed by a suitably-qualified member of the iCasework team, subject to the nature of the enquiry.

Change Requests

Change requests typically take two forms:

1. A request for a change to the software, by way of a software modification or enhancement requiring software development. Due to the nature of the iCasework platform, such requests are rare, since most requirements can be met through modification to the application configuration. However, if a request is identified as a re-

quest for a software change, there is a formal procedure that applies. This procedures is identified in the iCasework document "ISMS OP 37 – iCasework Software Change, Test and Release Process", embedded below.

2. A request for a change to the existing system configuration, for example, to modify an existing process or to develop a new process. The usual steps in such a circumstance (subject to the commercial arrangement in place between the parties) will be:

   a. Within 5 working days of the request being raised, discussion and agreement regarding a specification for the change, documented to the customer via a Statement of Works ("SoW").

   b. Agreement to and signature of the SoW by the client.

   c. Issue of a Purchase Order by the client, if required.

   d. Within 10 days of receipt of the signed SoW or Purchase Order (as appropriate), commencement of the necessary configuration activity. The scale of the activity will obviously depend upon the complexity of the requirement.

Training requests

The support team is available to assist any clients who have purchased the system and who have a current contract in place to resolve issues with their software. We do however stress that our support team is not able to provide training over the telephone or via email. If you require bespoke assistance with a module (for example, reporting) training is available to be purchased at a daily rate from our highly-trained consultants and many courses can be tailored to your own requirements.

Client responsibilities

The **System administrator** is responsible for first line support within the business and should carry out an initial assessment before a call is made to iCasework support team. This initial investigation will ensure that if the issue is a local issue (for example, a local networking issue) it is resolved by the client's IT support team. It is only when this process is exhausted that the issue should be raised in the iCasework support portal.

The supporting information that is provided to Civica about the issue is often key to resolving the problem. However, businesses must ensure that all personal information from any screenshots or other information provided to us has been redacted, blanked or removed in order to comply with Data Protection guidelines. If Civica deems it necessary to look at data on the live system, will require the specific agreement from the client to do so.

We have found that the following practices can help our Support team better understand your problem and more effectively respond to your concerns, as well as help you make the best use of your time:

- Submitting problems electronically
- Keeping the questions/issues separate (one problem per case)
- Specifying a priority based on your judgment of the business impact
- Keeping Civica support informed of major upgrades/implementations of your system
- Providing timely feedback on recommendations, so that the support team can close the support ticket when the problem has been resolved; if the problem reoccurs, you may reopen the original support ticket by resubmitting it electronically using the same reference number.

Information we require

General information

Organisations name	
Trading address including post code	
Contact in accounts responsible for invoices	
Address where invoices should be sent to	

Main Contact (System administrator or client nominated contact).

Name	
Job title	
Telephone	
Email	
Role	

Other contacts - Contact 2

Name	
Job title	

Telephone	
Email	
Role	

Other contacts - Contact 3

Name	
Job title	
Telephone	
Email	
Role	

Support outside UK business hours

Currently, our support team can be contacted by phone during UK Working Hours only. Outside these hours, issues should be submitted through our support portal. Our support portal is monitored 24/7 and issues submitted will be triaged by our support team.

Business critical issues

Business critical issues (those defined as priority 1 above) can also be reported through our help desk number by choosing option 4. Choosing this option will redirect you to our Out of Hours Service Desk, but we would ask customers to only choose this option after it has been established that the issue is indeed critical and not due to localised IT issues. We ask that customers undertake the following checks before contacting the Out of Hours Service Desk:

1. I'm unable to reach the login page:

Check that you can reach the login URL **https://[schema name].icasework.com/login**, if you cannot, proceed with checklist below:

1. Attempt to reach other web-based services (e.g. perform a google or bing search). If you are not able to reach other services, then your issue is likely to be localised. If other services do work, proceed to step 2:

2. Clear browser history (including cookies), restart browser and retry. If the symptoms remain the same, proceed to step 3:

3. Check with colleagues (preferably from different locations) that they are also unable to reach the login URL. If other colleagues are not having issues, then your issue is likely to be localised. If all users are unable to reach the login URL the issue should now be reported to Civica.

2. I can reach the login screen, but I'm unable to login to system:

Check you are using the correct login URL (**https://[schema name].icasework.com/login**), if you are using the correct URL, proceed with checklist below:

1. Clear browser history (including cookies), restart browser and retry. If the symptoms remain the same, proceed to step 2:

2. Check with colleagues (preferably from different locations) that they are also unable to login to the system. If other colleagues are able to login, then your issue is likely to be localised. If all users are unable to login, proceed to step 3:

3. Contact your network administrator to check if there is a problem with your local system login. Civica will redirect to this when "Single Sign-on" is implemented and this is

likely where the problem lies. If it has been established that the local login feature works, the issue should now be reported to Civica.

What to report:

Please provide the following information to your nominated representative for them to report when calling the Out of Hours Service Desk for iCasework:

1. Your organisation and contact details of relevant individuals (IT staff with a login to iCasework and familiarity with basic aspects of the system is preferential).

2. Details of when the problem first occurred or was first noticed, plus the number and duration of outages.

3. The number and locations of users known to be affected.

Service Level Agreement

This iCasework Service Level Agreement ("SLA") is a policy governing the use of the managed services provided via icasework.com ("iCasework") under the terms of the G-Cloud 12 Call Off Contract (“Agreement”) relating to the use of iCasework. This SLA applies separately to each account using iCasework. Unless otherwise provided herein, this SLA is subject to the terms of the Agreement. We reserve the right to change the terms of this SLA in accordance with the Agreement.

Definitions

“Agreement” means the G-Cloud 12 Call-Off contract between the parties.

"Outage" means a period when there is total loss of the Services.

"Quarterly Uptime Percentage" is calculated by subtracting from 100% the percentage of non-excluded downtime during the Service Period in which iCasework was in the state of "Unavailable." If you have been using iCasework for fewer than 90 days, your Service Period is the preceding 90 days, but any days prior to your use of the service will be deemed to have had 100% availability. Any downtime occurring prior to a successful Service Credit claim cannot be used for future claims. Quarterly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any iCasework SLA Exclusion (defined below).

“Scheduled Outage or Service Interruption” means an Outage or Service Interruption made by us when in our reasonable opinion such outage or interruption was necessary to facilitate improvements to or maintenance of the Services. We will use all reasonable endeavours to minimise such events and to schedule them at times which cause minimal disruption to service users.

“Service Commitment” means that we will use commercially reasonable efforts to make iCasework available with an Annual Quarterly Uptime Percentage (defined below) of at least 99% during each Service Period.

"Service Credit" is a British Pound credit, calculated as set forth below, that we may credit back to an eligible iCasework account, or make as a cash payment.

“Service Fee” means the fee payable annually in advance for the ongoing services delivery.

“Service Interruption” means a period during which there is partial loss of the Services.

“Service Period” means one of four periods, each of three calendar months in any calendar year, namely January-March, April-June, July-September and October-December.

“Services” means the professional services required to implement the solution together with the ongoing services required to deliver and maintain the solution.

"Unavailable" means the inability of a user of iCasework to retrieve or update case related information, provided that its account is active and in good standing i.e. the Service Fee and any other fees have been duly paid.

Service Commitment

Except where downtime results directly or indirectly from any iCasework SLA Exclusion (defined below), we will use commercially reasonable efforts to make iCasework available with a Quarterly Uptime Percentage of at least 99.5% during each Service Period. In the event iCasework does not meet the Quarterly Uptime Percentage commitment, you will be eligible to receive a Service Credit as defined below.

Service Credits

If your Quarterly Uptime Percentage drops below 99% for a Service Period, you will be eligible in full and final settlement for such deficiency to receive a Service Credit as per the measures set out below:

Quarterly Uptime Percentage Range	Service Credit Percentage
Greater than or equal to 99.00%	0%
97.50%-98.99%	2.50% of Service Fee x 25%
95.00%-97.49%	5.00% of Service Fee x 25%
Less than or equal to 94.99%	10.00% of Service Fee x 25%

Provided there is at least a further 12 months of your Agreement outstanding, we will apply any Service Credits against the next Service Fee due from you. Only in the final year of your Agreement will Service Credits entitle you to a refund from us. A Service Credit shall represent a genuine pre-estimate of loss in relation to a drop in your Quarterly Uptime Percentage.

Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Agreement, your sole and exclusive remedy for any unavailability or nonperformance of iCasework or other failure by us to provide iCasework is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA or termination of your use of iCasework in which case we would make a pro-rata refund of any Service Fee paid for any period beyond the effective date of termination in full and final settlement of any claim you might have in respect of such situation.

Notwithstanding the foregoing, if Unavailability meets or exceeds 10 percent (i.e., only 90 percent availability) at any time during any Service Period (each a "Chronic Outage"), you will be entitled to terminate the Agreement without penalty or further obligations to iCasework and will be entitled to a refund of amounts already paid for Services not yet received.

Credit Review and Payment Procedures

Quarterly Service Reviews will take place in the first month following the end of a Service Period. In most instances, Quarterly Service Reviews will be held remotely, but once a year, such reviews will take place face-to-face. No additional charge will be made by Civica UK Limited for its participation in or attendance at Quarterly Service Reviews.

The Quarterly Service Reviews will include a review of the Quarterly Uptime Percentage for the prior quarter. If the Quarterly Uptime Percentage as confirmed by us is less than 99% for the Service Period, then we will issue the Service Credit to you to be applied against the next Service Fee.

In the event that your Agreement has less than 12 months outstanding prior to expiry, any Service Credit will be made as a payment via bank transfer no later than in the third month of the Service Period subsequent to the Service Period to which the Service Credit applies.

iCasework SLA Exclusion

The Service Commitment does not apply to any unavailability, suspension or termination of iCasework, or any other iCasework performance issues:

(i) That result from a Scheduled Outage or Service Interruption

(ii) Customer requested Service Interruptions or Outages will be fulfilled but will not be considered a break in service by us and will not be considered when calculating breaches of the Service Level Agreement for any purpose or give rise to any liability on the part of us

(iii) We cannot control the flow of data beyond our internal network or on the Internet. We will use reasonable efforts to mitigate the impact of interruptions to the Services arising from events beyond our internal network but we disclaim any and all liability resulting from or related to such events.

(iv) We shall not be liable for any interruptions to the Services or Outages arising directly or indirectly from:

a. the effects of the failure or interruption of services provided by third parties; excluding AWS

b. Force Majeure

c. any actions or omissions by you (including, without limitation, breach of the Customer's obligations set out in this SLA, the Agreement or set out in a

Proposal or;

d. problems with the Customer's equipment and/or third party equipment;

e. interruptions to the Services requested by you.

(v) Arising from our suspension and termination of your right to use iCasework in accordance with the Agreement.

(vi) **Force Majeure**

a. Neither party hereto shall be liable for any breach of its obligations hereunder, except in respect of payment, resulting from causes beyond the reasonable control of the party in default (or its sub-contractors) including but not limited

to act of God, war, insurrection, riot, civil commotion, Government regulation, embargo, explosion, strike, labour dispute, , flood, fire or tempest (an “Event of Force Majeure”). Any time limit or estimate for a party to perform any act hereunder shall be suspended during an Event of Force Majeure.

b. Each of the parties hereto agrees to give notice forthwith to the other upon becoming aware of an Event of Force Majeure such notice to contain details of the circumstances giving rise to the Event of Force Majeure.

c. If a default due to an Event of Force Majeure shall continue for more than 30 days then the party not in default shall be entitled to terminate this Agreement. Neither party shall have any liability to the other in respect of the termination of this

Agreement as a result of an Event of Force Majeure but such termination shall not affect any pre-existing rights or obligations of either party.

Technical Support

We will provide your authorised account contacts with technical support on setting up and configuring your account, access to iCasework, and other issues related to the iCasework. Only your authorised account contacts may request information, changes or technical support. We allocate a severity status to all technical failures and aim to resolve the problem within the timescales given below. The actual response time will depend on the complexity of the issue and support request volumes at that time.

Category	Severity	Acknowledge	Resolve	KPI
P1	Critical – An issue which may result in the complete loss of the iCasework system (system down).	Within 30 minutes of the fault being raised	Within two hours of acknowledgement	95% of all requests per Service Period.
P2	Impaired – An issue that affects many users and disrupts the normal running of the system.	Within 60 minutes of the fault being raised	Within eight working hours of acknowledgement	90% of all requests per Service Period.
P3	Minimal - An	Within 8	Within five working	N/A
	issue that has minimal impact and does not affect the normal running of the system or for which a workaround is available.	Working Hours of the fault being raised. .	days of acknowledgement	

Data ownership

You own your data. If you ever decide to stop usage of iCasework, we will help you to get your data out of our systems, in accordance with our Exit Plan.

Exit Plan

We have a standard process for ensuring the orderly transfer of services to an alternate supplier, in the event of contract termination. You have contracted for a software as a service solution and retain no rights in our intellectual property, post-termination. Our obligations relate exclusively to the provision of your data, as maintained and managed within the iCasework solution.

The attached document from our Information Security Management System (reference ISMS OP 36, embedded below) details the off-boarding process:

1. In respect of the provision of the raw database disk (your entitlement to receive this at no additional cost being hereby confirmed), the elapsed time from commencement of service delivery to delivery of the data and associated documents is five working days.
2. Any professional services required of us to support you in migrating to an alternate supplier will be charged on a time and materials basis.
3. We will provide professional services within fifteen working days of receipt of written notice from you of your request for such services. The parties will agree the deliverables required from our activity so that both parties are clear of the scope of work – this will be documented in a Statement of Work ("SoW").
4. Any subsequent request for additional professional services that extend the current SoW or require a further SoW will be subject to the same fifteen working day leadtime before service delivery can commence.
5. It is expected that any data extracted from the iCasework system will be imported into a new system procured by you from an alternate supplier. The responsibility for quality assurance of the extracted data (regardless of the mechanism employed for data extract) rests with you and your new new supplier.
6. It is your responsibility (working with your new supplier) to request professional services from us in good time to ensure that all migration activities are completed in advance of the Agreement end-date.

iCasework

ISMS OP 36

Client Off Boarding Procedure

Document Number	ISMS OP 36
Document Name	Client Off Boarding Procedure
Approved by	Shine Prakash
Reviewed and Approved	March 2019
Version Number	V11
Review Date	February 2020
Document Index updated?	Yes
Old Version Archived?	Yes
Classification	Company Confidential

Service Reliability Measures

In addition to the standard helpdesk metrics that report upon call volumes, priorities and call resolution against contractual SLA, Civica will supply the following service reliability measures:

- Number of minor security breaches (a “minor” breach is defined as a breach not considered to require reporting to the ICO)
- Number of major security breaches (a “major” breach is defined as a breach considered to require reporting to the iCO)
- System Availability (uptime) - access to a real-time reporting tool is made available to all iCasework users

We do not offer reports on security updates implemented versus those that should have been implemented; if an update is fundamental to system security, it will be implemented

Appendix Two

High Level on Boarding plan

The following is a high-level summary of the project activities and timeline. This is subject to further discussion and confirmation.

For reference owners of activities are defined as follows

JOINT CL = Civica and MOJ/OSPT resource with Civica having lead responsibility and MOJ providing input

JOINT = Civica and MoJ jointly responsible

CGI = CGI technical resource

Customer = MOJ/OSPT resource

CIVICA = Civica resource

Timeline

Activity	Owner	M1	M2	M3	M4	M5	M6	M7	M8	M9
Stage 1 - Commencement										
Scope agreed for project	**JOINT**									
Timeframes agreed	**JOINT**									
Project roles identified and appointed	**JOINT**									
Project and product documentation distributed	**CIVICA**									
Detailed timeframes agreed	**JOINT**									
Stage 2 – Scoping										
Review of requirements	**JOINT CL**									
Agreed workflow requirements	**JOINT CL**									
Agreed	**JOINT CL**									

functional requirements										
Agreed technical requirements	**JOINT CL**									
Agreed scope documented and distributed	**JOINT CL**									
Reporting requirements detailed	**JOINT CL**									
Agreed integration requirements	**JOINT CL**									
UAT System create and access given	**CIVICA**									
Stage 3 – Super user training										
Project team front end training	**JOINT CL**									
Reference data training(Clients / Teams / Work areas)	**JOINT CL**									
Time setup training	**JOINT CL**									
Billing and Disbursments setup training	**JOINT CL**									
Template training	**JOINT CL**									
Case and fields setup training	**JOINT CL**									
Workflow setup training	**JOINT CL**									
Stage 4 - Configuration and Setup										
Setup / Import of clients / teams / work areas	**Customer**									
Setup of time recording	**Customer**									
Setup of billing and disbursements	**Customer**									
Workshops on case and workflow setup	**JOINT CL**									
Setup of standard process	**JOINT CL**									
Setup of required fields	**JOINT CL**									

Setup of required roles	**JOINT CL**									
Setup of merge templates	**Customer**									
Setup of workflows (Workflows TBC)	**JOINT CL**									
Setup of security and authorisation groups	**JOINT CL**									
Setup of retention policies	**JOINT CL**									
Stage 5 – Technical Integration										
Business requirements agreed	**JOINT CL**									
Technical documentation sent and reviewed	**JOINT CL**									
Technical integration elements setup	**JOINT CL**									
Setup of EUAT system for technical testing	**JOINT CL**									
Stage 6 – Trial data migration										
Elements required for trial migration setup	**JOINT CL**									
Mapping for trial migration	**JOINT CL**									
Upload database for trial conversion	**CGI**									
Upload documents for trial conversion	**CGI**									
Trial conversion	**CIVICA**									
Trial migration made available for testing	**CIVICA**									
Stage 7 - Testing										
Testing of system	**Customer**									
Testing of migrated data	**Customer**									
Testing of standard process	**Customer**									
Testing of email	**Customer**									
Testing of SSO	**Customer**									

Testing of templates	**Customer**									
Testing of core functionality	**Customer**									
Testing of case and workflow	**Customer**									
Testing of integration elements	**JOINT**									
Review following initial testing	**Customer**									
Feedback as to the testing	**Customer**									
Actions following testing feedback	**JOINT**									
Further testing performed	**Customer**									
Stage 8 - Pre Go Live										
Reports and bundles training	**JOINT CL**									
Setup of bundle structures	**Customer**									
Customer to test bundle structures	**Customer**									
Setup of required reports	**Customer**									
Sign off on functionality	**Customer**									
Sign off on technical integration	**Customer**									
Sign off on processes	**Customer**									
Sign off on migration	**Customer**									
Sign off on integration	**Customer**									
Proceed to go live Gate	**JOINT**									
Stage 9 - Go Live										
Project team end user training	**JOINT CL**									
End user training	**JOINT CL**									
Upload database for live conversion	**CGI**									
Upload documents for live conversion	**CGI**									
Live conversion	**CIVICA**									
Go Live	**JOINT CL**									

Go Live Floorwalking	**JOINT CL**									
Post Go Live Floorwalking	**CIVICA**									
Post Go Live Services Support	**CIVICA**									
Sweep-Up	**CIVICA**									
Stage 10 - Project Completion										
Handover to Support	**CIVICA**									
Project closure meeting	**JOINT CL**									
Project completed	**JOINT**									

Key activities

Implementation Services Project Milestone	Projected date
Project kick off and provision and deployment of core platform for design and configuration. Detailed project plan including agreed UAT and Sign off processes agreed	30/05/2021
Design and configuration phase	30/06/2021
Sign off of Test migration	30/07/2021
UAT Sign off of configuration and design	14/08/2021
End user training and go live	30/08/2021
Post go live configuration eg Client Portal	30/10/2021

Key Dependencies

1. Availability of Civica, MOJ/OSPT and CGI resources to support key activities. Specifically, availability of OSPT resources to support UAT testing and availability of CGI to support test and live data uploads to migration platform within desired timescales

Risks

Risk	Mitigation	Impact
Delay to project timescales due to time required for CGI to provide data for migration	Reschedule project	Delayed go live with need to consider continued use of current Casper system beyond 31/08/2021 MOJ to agree contract extension with CGI for an agreed term on a pro rata basis.
Data upload for migration takes longer than expected	Adjust project schedule	Delayed go live with need to consider continued use of current Casper system beyond 31/08/2021
Civica Project Team members unavailable	Allocated alternative Civica Staff to project	Low impact, alternative resources are available and can be allocated at relatively short lead time
OSPT Project team members not available	Alternative staff allocated	Possible

Appendix Three –

Official Solicitor & Public Trustee Procurement of Case Management System

Functional and Non-Functional Requirements

1. Background

i. The Office of the Official Solicitor and Public Trustee (OSPT) is an associated office of the Ministry of Justice. OSPT was created in 2001 with the merger of the Official Solicitor's Office and the Trust Division of the Public Trust Office. The Official Solicitor acts for people who lack the capacity to conduct their own litigation and no other suitable person is able and willing to act. He usually becomes formally involved when appointed by the Court, and he may act as his own solicitor, or instruct a private firm of solicitors to act for him.

Functions undertaken in England and Wales:

- acting as litigation friend of minors or adults who lack litigation capacity in county court or High Court proceedings in England and Wales, and in the Court of Protection (CoP),
- acting as Advocate to the Court in the High Court and the CoP;
- acting as last resort personal representative of the estate of a deceased person, or trustee of a trust, or financial deputy under the MCA 2005.

Functions undertaken to fulfil international obligations:

- child abduction and contact matters are handled by the International Child Abduction and Contact Unit (ICACU) on behalf of the Lord Chancellor who is the Central Authority for England and Wales;
- Reciprocal Enforcement of Maintenance Orders Unit (REMO) handles, again for the Lord Chancellor, the sending and receiving of applications for maintenance enforcement where one of the parties lives outside the United Kingdom.

2. Objectives, Budget and Timeline

i. Casper is a Commercial off the Shelf (COTS) Case Management Tool (CMT) used by the Official Solicitor and Public Trustee (OSPT) to track all litigation matters. Casper was implemented in April 2010 and was designed to be a land based system. It is provided by Civica using their Norwel Prescient package and

is hosted by CGI. CGI also manages incident resolution via the CGI AMS contract. However these incidents, that average 10 per month, are in the main resolved by OSPT support staff, Civica or Vodafone.

ii. There are circa 150 registered user accounts for the CMT.

iii. The OSPT needs to procure a replacement IT Solution to manage its caseload, due to the pending termination of the CGI hosting contract, which hosts the current Case management system Casper. The current system is over 10 years old, and whilst there were no plans to replace the existing system prior to the notification of the CGI hosting contract end date of March 2022. This is an ideal time and opportunity to review the current system against existing requirements. The current supplier has confirmed that they have since created a next generation, improved case management system, since the creation of Casper.

iv. MoJ digital teams will be working with the OSPT to provide advice and guidance on adopting a tool that is both fit for purpose and in line with the Strategic direction of the MOJ.

v. Whilst the Authority does not wish to prescribe a solution or approach, it is anticipated that a CoTS package will be the natural fit, although that shouldn't prevent potential suppliers from suggesting other options based upon a real understanding of the OSPT's requirements and without a burdensome or unrealistic price tag.

vi. The Potential Supplier would be expected to include all costs associated with each provision. All costs should be included within Pricing Matrix

vii. The CMS needs to be delivered before the end of the financial year. March 2021. Whilst a CoTS package is the most likely solution, the new supplier will need to build the workflows and ensure it integrates with any other OSPT systems. It is therefore desirable to have the new supplier on board by January 2021.

3. Security Classification

Data will be held securely in accordance with HMG and OSPT policy regarding Information Assurance. The Protected marking is assessed as Official.

4. Who will be using the application?

The solution will be accessed by approximately 140 OSPT users. The solution must have the ability to scale up and scale out to meet future business requirements.

5. Requirements Scope

The new solution will provide the following according to the more detailed functional and non-functional requirements;

Case Management Application

Including:

a) Case information;
b) Email Integration with MS Outlook
c) Interface with Word and Excel to provide Document management Functionality
d) Workflows;
e) Time Recording
f) Reporting;

g) Dash boards for user and management KPI reporting and workload monitoring.

h) Billing
i) Fee/Cost/Disbursement recording
j) Client accounting (Financial Management)
k) Search;
l) EDRM Management; Not sure what this is?

m) Security (End User)
n) Auditing
o) Archiving & GDPR functionality - Ability to archive and permanently delete information, in line with data retention guidelines.

6. Business Process

Litigation Services

The OSPT litigation services are delivered by 4 teams, each of which manages a distinct area of work. In all cases, my aim as Official Solicitor is to protect the interests of the vulnerable party for whom I am acting:

- **Civil Litigation** – The OS acts as litigation friend for the protected party in all types of cases brought in the civil courts. These cases include possession (L&T) claims in which the protected party is usually the defendant, damages claims against Local Authorities (usually on behalf of children), Judicial Reviews and cases brought under the HRA.
- **Family Litigation** – The OS acts as litigation friend in these cases for the parent(s) who lacks capacity (in the case of public and private law children act cases) and for the incapacitated party to divorce proceedings.
- **Court of Protection**: **Property and Affairs Litigation** – The OS acts in these cases as both litigation friend and solicitor for 'P' (the subject of the litigation) on the invitation of the Court of Protection. The OS charges for the work done on these cases.
- **Court of Protection: Healthcare and Welfare Litigation** – in all of these cases the OS is invited to act by the Court of Protection. In the majority of the cases external solicitors are instructed, however a small number of cases (mainly urgent medical treatment cases) the OS also acts as solicitor. The OS charges for the cases where we act as solicitor.

Trusts and Estates

The trusts and estates that the OSPT administer, as either Official Solicitor or as Public Trustee are managed by the Trusts and Estates team. There is a strict last resort policy and it is rare that the office accept new cases; any new cases will usually be trusts created for the administration of an award made by the Criminal Injuries Compensation Authority where there is no other person suitable to manage the award. In these and other trusts and estates cases, the OS's role is to manage the assets under her control in the interests of vulnerable individuals or persons under disability.

The Public Trustee is Custodian Trustee and an Administrative Trustee of the Chequers Estate Trust and as such as a member of the Chequers' Board of Trustees.

Public Trustee records (for a fee) of applications for Notice to quit under the Law of Property (Miscellaneous Provisions) Act 1994 which are served on property originally occupied by someone who is now deceased and for whom personal representatives are not acting.

International Teams

The International Child Abduction and Contact Unit (ICACU) which carries out in England and Wales the operational functions of the Lord Chancellor who is the Central Authority under The Hague and European Conventions on child abduction, contact and protection.

The Reciprocal Enforcement of Maintenance Orders Unit (REMO) which carries out in England and Wales the operational functions of the Lord Chancellor who is the Central Authority for establishment and enforcement of international maintenance claims.

7. Functional Requirements

The detailed requirements are listed below and have been assessed for their suitability and priority using the following criteria:

Conventions

Priorities have been assigned to requirements using the MoSCo convention as follows:
M = Must - Mandatory requirement
S = Should - Highly desirable requirement
C = Could - Desirable requirement

Further volumetric and statistical information can be found in the Non-Functional Specification.

Case Management Application

No	Products	Requirements	M/S/C	Response
FC1	Case	The case solution must be able to allocate a unique reference/case number/case type.	**M**	

FC2		The case solution must enable the Authority to create, edit, view, delete and override case details/notes/criteria	**M**	
FC3		The case solution must provide the facility for Case Managers to be able to organise and manage cases for which they have responsibility.	**M**	
FC4		The case solution must provide an easy to navigate user interface, using language that will be familiar to OSPT staff.	**M**	
FC5		The case solution should be able to generate correspondence via email and print.	**M**	
FC6		The case solution must provide contextual help to users such as system and process functions. This help should be business configurable	**M**	
FC7		The case solution must enable cases to be linked by reference number.	**M**	
FC8		The case solution must enable the upload of documents in various formats including any meta data associated with the document.	**M**	
FC9		The case solution should flag inbound communications from OSPT users	**S**	
FC10		The case solution should be able to recognise and automatically assign and update status according to events	**S**	
FW1	**Workflows**	The case solution must enable the Authority to manage its business process through a series of manual and automated steps. Referred to as workflows	**M**	
FW2		The case solution must have the ability to escalate notifications	**M**	
FW3		The case solution must be able to create criteria based events and event driven activities/tasks	**M**	
FW4		The case solution must track and report on case progress or status	**M**	
FW5		The case solution should create case status notifications and warnings and inform users and customers when deadlines are due via an in-application dashboard.	**S**	
FW6		The case solution should give the user the ability to customise who receives notifications (internal and external), ideally with use of a prompt	**S**	

FW7		The case solution should enable automatic allocation of activities/tasks to specific users and business groups	**S**	
FR1	**Reporting**	The solution must have a built-in reporting tool which will enable end users to report on case data	**M**	
FR2		The reporting solution must enable the Authority to build, configure and store reports, with all available case data	**M**	
FR3		The reporting solution must provide standard and ad hoc reports in live and historical data at any time	**M**	
FS1	**Search**	The case solution must include an integrated search function which will enable the Authority to find and search records and data using a comprehensive variety of criteria.	**M**	
FS2		The search function must enable users to search using single or multiple fields	**M**	
FS3		The system must enable users to search for electronic documents stored against a case record using existing metadata.	**M**	
FD1	**Data Management**	The solution must provide archive functionality for case records and enable the authority to comply with GDPR regulations	**M**	
FSEU1	**Security (End User)**	The case solution must enable the Authority to set, assign or remove appropriate user permission levels	**M**	
FSEU2		The case solution must allow passwords to be created and reset by the user within parameters set by the authority	**M**	
FSEU3		The case solution must allow the Authority to set, assign or remove appropriate case access levels and apply the principle of least privilege for all data access. This means restrict by data content, and restrict to read-only rather than read-write wherever possible and appropriate	**M**	
FSEU4		The case solution must ensure unique per-user accounts.	**M**	
FA1	**Audit**	The case solution must log specific transactions including viewing and editing of data as defined by the Authority	**M**	
FA2		The case solution must date/time stamp all activities that occur	**M**	

FA3		The data management function must enable permitted users to access and view audit logs	**M**	
FA4		The data management functions must provide the ability to archive historical data automatically according to the Authorities' criteria.	**M**	
FA5		The data management functions must provide the ability to roll back user actions and changes for example a mistaken deletion of data	**M**	
FA6		logs and other auditable material must be stored remotely to ensure forensic diagnosis capability following incident	**M**	

Hosting and Infrastructure

No	Products	Requirements	M/S/C	Response
FHI1	**Hosting and Infrastructure**	The Case Management Solution must be hosted within Public Cloud in line with MoJ's requirements for OFFICIAL data (https://ministryofjustice.github.io/security-guidance/mythbusting/data-sovereignty/#data-sovereignty)	**M**	
FHI2		The hosting solution must comply with the Authority's Business Continuity Plan and in the event of disaster within the hosting environment that functionality and data can be recovered in under 8 hours. (operational backups are covered in NFDR4)	**M**	
FHI3		The hosting solution must be able to be accredited to appropriate NCSC Security Guidance	**M**	
FHI4		The hosting environment must facilitate the capacity to support interfaces and data flows to and from integrated systems	**M**	
FHI5		The solution must be accessed by the OSPT customers, from the public Internet using web browsers via HTTPS. Browsers should be supported, E11 and FF68.1 and all modern browsers	**M**	

FHI6		The hosting environment must: ● Support the anticipated performance load ● Provide antivirus software and services for the solution hosting environment. ● Provide sufficient storage capacity to manage the expected requirements ● Provide management information to enable the Authority to understand how its systems are being utilised	**M**	
FHI7		The hosting solution must be able to deliver satisfactory response times on the existing / planned MoJ's network	**M**	
FHI8		The solution must be capable of working with standard monitoring and systems management tools	**M**	
FHI9		The application must have an availability level at the data centre of least 98.9% per year (Planned outages excepted)	**M**	
FHI10		The hosting solution should offer a flexible processing and storage capacity – such that the Authority only bears charges for the capacity utilised and consumed	**S**	

Systems Integration

No	Products	Requirements	M/S/C	Response
FSYI1	**Systems Integration**	The supplier must ensure that all the components of the solution work seamlessly together to create an efficient and effective monitored end-to-end solution.	**M**	
FSYI2		The supplier must ensure that all elements of the solution will: Integrate with any enterprise based Active Directory structure to enable single sign-on).	**M**	

		Integrate with MS standard Office tools. Integrate with the CAT? Integrate with a range of different published APIs?		

Service Integration and Management (SIAM)

No	Products	Requirements	M/S/C	Response
FSIN 1	**Service Integration**	The supplier must document all aspects of Architectural Governance including implementation of a system of controls over the creation and monitoring of all architectural components and activities, and ensuring compliance with the Authority's standards.	**M**	
FSIN 2		The supplier must ensure that their Service Design Standards conform to the Cabinet Office Service Design and Delivery Guide.	**M**	
FAS 1	**Application Support**	The supplier must supply 2nd and 3rd line application support (first line to be performed by MoJ Technology Service Desk)	**M**	
FAS 2		The supplier must ensure application support is available to the Authority during working hours, as outlined under the relevant Service Level Agreement.	**M**	
FAS 3		The supplier must service levels and work with the authority to deliver improvements	**M**	
FAS 4		The supplier should create and maintain detailed and accurate end-to-end Service Level Agreement reporting, and will use this data to provide management information to the Authority and to initiate service improvement actions.	**S**	
FET E1	**End to end Business Process Management**	The supplier must supply and maintain a comprehensive plan and service for: Incident Management Problem Management Event Management Continuity Management Availability Management Change Management Release Management	**M**	

		Security Management		

9. Non-Functional Requirements

The detailed requirements are listed below and have been assessed for their suitability and priority using the following criteria:

Conventions

Priorities have been assigned to requirements using the MoSCo convention as follows:
M = Must - Mandatory requirement
S = Should - Highly desirable requirement
C = Could - Desirable requirement
Non-Functional Requirements

No	Products	Requirements	M/S/C	Response
NFI1	**Interoperability**	Integration with third-party applications or services must take place over open standards such as TCP/IP, HTTP, JSON/JSONP or XML. ?	**M**	
NFI2		Interfaces with internal and external parties must comply with HMG standards.	**M**	
NFL1	**Legal and Regulatory**	The supplier must ensure that any solution (technical or business process) adheres to OSPT Legislation). For example, the solution must not be designed in such a way that it limits or allows certain practices or processes which impact the role of the OSPT	**M**	

NFL2			The solution must adhere to the Equalities Act and be able to support Assistive Technology Users.	**M**	
NFL3			The solution must adhere to General Data Protection Regulations (GDPR)	**M**	
NFH1		**Hours of Operation**	OSPT users typically work between the hours of 7am and 7pm, Mondays to Fridays but should be available outside of these hours		
NFH2			Some weekend working does take place within the sites but on a limited scale.		
NFA1		**Accessibility**	The solution must comply with the Disability and Equality Act.	**M**	
	NFCS 1	**Capacity and Scalability**	The solution must be capable of supporting 200 concurrent users consuming system resources at any one time. The solution must be scalable if the authority increases the number of users.	**M**	
	NFCS 2		The solution must be able to support an average of 120 new cases per day and be able to flex to support spikes in demand and other workload fluctuations.	**M**	
	NFAV 1	**Availability**	The application must have an availability level at the data centre of least 95% per year (Planned outages excepted)	**M**	
	NFAV 2		The solution must provide business continuity in the event of a failure.	**M**	
	NFS1	**Security**	The solution must adhere to HMG Security Policy Framework guidelines.	**M**	

	NFS2		The solution supplier must define, document and agree with the Authority the roles and responsibilities of their staff and sub-contractors whom are responsible for administering and operating the solution.	**M**	
	NFS3		All staff and sub-contractors must be cleared to SC level.	**M**	
	NFS4		The solution supplier must ensure that all users and relevant employees have their solution access rights revoked on termination of employment.	**M**	
	NFS5		The solution supplier must ensure that all solution information and assets and supporting utilities are provided appropriate physical protection from internal, external and environment threats.	**M**	
	NFS6		The solution supplier must ensure solution supporting utilities (hardware, firmware and software including hosting) are maintained and patched up-to-date, preventing loss or interruption of services.	**M**	
	NFS7		The solution supplier must define, document, agree with the Authority and regularly maintain (at least annually) Standard Operating Procedures for solution administration and maintenance, in line with the support and accreditation requirements.	**M**	
	NFS8		The solution supplier must ensure that their business continuity and disaster recovery arrangements conform to the Authority's business continuity plans.	**M**	

	NFS9		The supply must provide protective monitoring to support the detection of malicious activity. This should include: ● Network enterprise event monitoring ● Application management ● Hosting Enterprise Event Monitoring	**M**	
	NFS10		The solution must provide controls that prevent log information from being modified.	**M**	
	NFS11		The solution supplier must ensure their staff that are solution users have their access rights periodically reviewed and when a user role changes.	**M**	
	NFS12		The solution must suspend or shut down its sessions after a pre-defined period of inactivity	**M**	
	NFS13		The solution supplier must ensure that the solution is appropriately isolated from their other customer environments.	**M**	
	NFS14		The solution software and firmware components must have full vendor support arrangements (security and general fixes).	**M**	

	NFS15		The solution software and firmware components within the live, DR and NLE/Test environments must be patched up-to-date, in line with the patch management policy to prevent consumers from exploiting technical vulnerabilities	**M**	
	NFS16		The solution must have any technical vulnerabilities identified from a penetration test treated (reduced, avoided, transferred or accepted) at intervals of not more than 12 calendar months since the last successful tests before any major change to infrastructure goes live, including but not limited to modifications to functional capability, implementation, or hosting any issues identified during Penetration tests or IT Health Check as a result of service changes must be mitigated or accepted before the service changes go live	**M**	
	NFS17		The solution supplier must respond to incidents and report on incidents as specified within the incident management plan.	**M**	
	NFS18		The solution supplier must document, implement and regularly test and review business continuity arrangements for their facilities, utilities, and systems that support the solution.	**M**	
	NFS19		The solution supplier should ensure that OSPT Protectively Marked information or personal information is not processed on development and test environments.	**S**	
	NFS20		The solution supplier should have an Information Security Policy that reflects the control objectives as specified within the ISO27001 control set.	**S**	

	NFS21		The solution supplier should ensure that their development and test environments are appropriately separated from the live environment.	**S**	
	NFS22		The authority requires Cyber Essentials Plus (commonly 'CE+') certification and it is highly recommended that suppliers have NCSC Commercial Product Assurance (CPA) https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa for their products or services. If the tool chosen is cloud based, the authority would also be looking for alignment with NCSC Cloud Security Principles https://www.ncsc.gov.uk/collection/cloud-security	**M**	
	NFS23		The solution must enforce Multi-factor authentication (MFA) access controls	**M**	
	NFS24		All data must be encrypted at rest and in transit.	**M**	
	NFDO1	**Documentation**	Supplier should provide a High-Level and Low-Level Design documenting the proposed solution. This should include: Data Dictionary Reference to API Schemer Security Policy Service Level Agreements	**S**	

			Training Guides Evidence of Accreditation		
	NFDE 1	**Delivery**	The Solution delivery project manager must work with the team nominated by the Authority and report against agreed delivery milestones aligning with the overall project delivery plan and business change implementation plan.	**M**	
	NFDE 2		The supplier is expected to provide project management and resources for the delivery of the solution	**M**	
	NFT1	**Training**	The Supplier must provide training and training courseware and system administrator guidance notes to users in training workshops, which can then be re-used by the Authority under a 'train the trainer' model	**M**	
	NFM1	**Monitoring**	Data reporting must not affect performance of the production service.	**M**	
	NFM2		The supplier must provide performance reports providing information on: • Business transaction volumes • Computational transaction volumes • User concurrency • End-to-end transaction times • Data centre boundary transaction times • Application availability • Breakdown of server availability • Capacity should be produced monthly	**M**	

	NFR1	**Resilience**	The application must not have a single point of failure within the data centre. All application components within that data centre should be duplicated or have some form of failover	**M**	
	NFR2		In the event of an application component failover, the application must still be capable of supporting the defined peak load.	**M**	
	NFR3		The application's disaster recovery facility must be equal to the application's live facility both in terms of access to the data and capacity.	**M**	
	NFR4		The application backup must be tested at least once a year through a full backup restoration exercise. Details of the test and results to evidence success should be agreed with the authority	**M**	
	NFR5		In the event of the loss of a single data centre: ● The application should be online within 8 working hours. ● Data loss must be restricted to the last 30 minutes of transactional activity	**S**	
	NFLG 1	**Logging**	Log files must not be allowed to grow to the extent that they affect system performance.	**M**	

	NFLG 2		In the event of an error, the application log file should provide enough information for support teams to isolate the point and possible cause of failure.	**S**	
	NFD R1	**Data Retention and Backup**	The solution must be incrementally and completely backed up at intervals appropriate to ensure business continuity.	**M**	
	NFD R2		The solution must be accompanied by a data restoration plan. This plan will encompass foreseen maintenance tasks such as replacing hardware, or rebuilding/modifying/replacing the operating system; as well as unforeseen events such as system failures or power outages.	**M**	
	NFD R3		The application must hold data only for as long as is specified by the data retention schedule as specified by the Authority.	**M**	
	NFD R4		All server volumes should be stored and replicated. The snapshot frequency should be applied to all volumes as follows: ● Every 2 hours with a 24-hour retention ● Nightly with a 7-day retention ● Weekly on a Sunday with a 2-week retention	**S**	
	NFD R5		The restoration of data should take no longer than 1 working day from the point of the request being made.	**S**	

	NFD R6		Cached or 'past expiry' data must be purged as soon as possible, unless subject to a Retention Order, as specified by the authority.	**M**	
	NFTE 1	**Testing**	The solution must provide a non-live environment which can be used for development and testing.	**M**	
	NFTE 2		The non-live environment must be updated and be an accurate representation of the live system in terms of patching and security processes.	**M**	
	NFTE 3		The supplier must provide and execute full testing.	**M**	
	NFTE 4		The supplier must provide and execute security tests that prove users can only access authorised data and functionality.	**M**	
	NFTE 5		The supplier must support User Acceptance Testing	**M**	
	NFTE 6		The supplier must document all testing for audit and customer acceptance	**M**	

	NFSS 1	**System Support**	The solution must be accompanied by a support plan that describes the technical and managerial processes necessary to support the solution once operational.	**M**	
	NFSS 2		The support plan must include a description of the support personnel and their roles, as well as the processes to resolve problems arising within the solution boundaries, and escalation policies.	**M**	
	NFSS 3		The support plan must include service support hours and response times to calls.	**M**	
	NFSS 4		The support plan must include details of third party maintenance service levels and agreements including any OWA's	**M**	
	NFE1	**Exit**	As far as possible, the supplier must provide upfront costs of exit at the conclusion of the contract.	**M**	
	NFE2		The supplier must provide a documented method for data extraction at the conclusion of the contract and data deletion using an NCSC approved standards (https://ministryofjustice.github.io/security-guidance/#data-destruction)	**M**	

Appendix Four

Civica Response to Official Solicitor & Public Trustee Procurement of Case Management System

Functional and Non-Functional Requirements

Civica UK Ltd:
Response to a
Request for Information (RFI)

Official Solicitor & Public Trustee Procurement of Case Management System

Functional and Non-Functional Requirements

25th January 2021

Contents

1. Background

i. The Office of the Official Solicitor and Public Trustee (OSPT) is an associated office of the Ministry of Justice. OSPT was created in 2001 with the merger of the Official Solicitor's Office and the Trust Division of the Public Trust Office. The Official Solicitor acts for people who lack the capacity to conduct their own litigation and no other suitable person is able and willing to act. He usually becomes formally involved when appointed by the Court, and he may act as his own solicitor, or instruct a private firm of solicitors to act for him.

Functions undertaken in England and Wales:

- acting as litigation friend of minors or adults who lack litigation capacity in county court or High Court proceedings in England and Wales, and in the Court of Protection (CoP),
- acting as Advocate to the Court in the High Court and the CoP;
- acting as last resort personal representative of the estate of a deceased person, or trustee of a trust, or financial deputy under the MCA 2005.

Functions undertaken to fulfil international obligations:

- child abduction and contact matters are handled by the International Child Abduction and Contact Unit (ICACU) on behalf of the Lord Chancellor who is the Central Authority for England and Wales;
- Reciprocal Enforcement of Maintenance Orders Unit (REMO) handles, again for the Lord Chancellor, the sending and receiving of applications for maintenance enforcement where one of the parties lives outside the United Kingdom.

2. Objectives and Timeline

i. Casper is a Commercial off the Shelf (COTS) Case Management Tool (CMT) used by the Official Solicitor and Public Trustee (OSPT) to track all litigation matters. Casper was implemented in April 2010 and was designed to be a land-based system. It is provided by Civica using their Norwel Prescient package and is hosted by CGI. CGI also manages incident resolution via the CGI AMS contract. However, these incidents, that average 10 per month, are in the main resolved by OSPT support staff, Civica or Vodafone.

ii. There are circa 150 registered user accounts for the CMT.

iii. The OSPT needs to procure a replacement IT Solution to manage its caseload, due to the pending termination of the CGI hosting contract, which hosts the current Case management system Casper. The current system is over 10 years old, and whilst there were no plans to replace the existing system prior to the notification of the CGI hosting contract end date of March 2022. This is an ideal time and opportunity to review the current system against existing requirements. The current supplier has confirmed that they have since created a next generation, improved case management system, since the creation of Casper.

iv. MoJ digital teams will be working with the OSPT to provide advice and guidance on adopting a tool that is both fit for purpose and in line with the Strategic direction of the MOJ.

v. Whilst the Authority does not wish to prescribe a solution or approach, it is anticipated that a CoTS package will be the natural fit, although that shouldn't prevent potential suppliers from suggesting other options

based upon a real understanding of the OSPT's requirements and without a burdensome or unrealistic price tag.

vi. The Potential Supplier would be expected to include all costs associated with each provision. All costs should be included within Pricing Matrix

vii. The CMS needs to be delivered before the end of the financial year. March 2021. Whilst a CoTS package is the most likely solution, the new supplier will need to build the workflows and ensure it integrates with any other OSPT systems. It is therefore desirable to have the new supplier on board by January 2021.

3. Security Classification

Data will be held securely in accordance with HMG and OSPT policy regarding Information Assurance. The Protected marking is assessed as Official.

4. Who will be using the application?

The solution will be accessed by approximately 140 OSPT users. The solution must have the ability to scale up and scale out to meet future business requirements.

5. Requirements Scope

The new solution will provide the following according to the more detailed functional and non-functional requirements;

Case Management Application

Including:

a) Case information;
b) Email Integration with MS Outlook
c) Interface with Word and Excel to provide Document management Functionality
d) Workflows;
e) Time Recording
f) Reporting;

g) Dash boards for user and management KPI reporting and workload monitoring.

---

h) Billing
i) Fee/Cost/Disbursement recording
j) Client accounting (Financial Management)
k) Search;
l) Data Management;

m) Security (End User)
n) Auditing
o) Archiving & GDPR functionality - Ability to archive and permanently delete information, in line with data retention guidelines.

6. Business Process

Litigation Services

The OSPT litigation services are delivered by 4 teams, each of which manages a distinct area of work. In all cases, my aim as Official Solicitor is to protect the interests of the vulnerable party for whom I am acting:

- **Civil Litigation** – The OS acts as litigation friend for the protected party in all types of cases brought in the civil courts. These cases include possession (L&T) claims in which the protected party is usually the defendant, damages claims against Local Authorities (usually on behalf of children), Judicial Reviews and cases brought under the HRA.
- **Family Litigation** – The OS acts as litigation friend in these cases for the parent(s) who lacks capacity (in the case of public and private law children act cases) and for the incapacitated party to divorce proceedings.
- **Court of Protection**: **Property and Affairs Litigation** – The OS acts in these cases as both litigation friend and solicitor for 'P' (the subject of the litigation) on the invitation of the Court of Protection. The OS charges for the work done on these cases.
- **Court of Protection: Healthcare and Welfare Litigation** – in all of these cases the OS is invited to act by the Court of Protection. In the majority of the cases external solicitors are instructed, however a small number of cases (mainly urgent medical treatment cases) the OS also acts as solicitor. The OS charges for the cases where we act as solicitor.

Trusts and Estates

The trusts and estates that the OSPT administer, as either Official Solicitor or as Public Trustee are managed by the Trusts and Estates team. There is a strict last resort policy and it is rare that the office accept new cases; any new cases will usually be trusts created for the administration of an award made by the Criminal Injuries Compensation Authority where there is no other person suitable to manage the award. In these and other trusts and estates cases, the OS's role is to manage the assets under her control in the interests of vulnerable individuals or persons under disability.

The Public Trustee is Custodian Trustee and an Administrative Trustee of the Chequers Estate Trust and as such as a member of the Chequers' Board of Trustees.

Public Trustee records (for a fee) of applications for Notice to quit under the Law of Property (Miscellaneous Provisions) Act 1994 which are served on property originally occupied by someone who is now deceased and for whom personal representatives are not acting.

International Teams

The International Child Abduction and Contact Unit (ICACU) which carries out in England and Wales the operational functions of the Lord Chancellor who is the Central Authority under The Hague and European Conventions on child abduction, contact and protection.

The Reciprocal Enforcement of Maintenance Orders Unit (REMO) which carries out in England and Wales the operational functions of the Lord Chancellor who is the Central Authority for establishment and enforcement of international maintenance claims.

7. **Instructions on how to complete Functional and Non-Functional questions;**

The supplier is asked to complete Functional (Table 2 and Non- Functional (Table 3) Requirements table to indicate how your services offering meet our requirements

Please complete by using YES (Y), NO (N) or Partial (P). Where you provided 'P' as your response, please explain.

In addition, Table 4 includes a set of questions for you to complete.

The Authority will base the selection criteria on Most Technical Advantage Tender (MEAT) to determine our best fit

Your final response would need to be received **on or before 15:00 25th January 2021**

8. **Indicative Timeline -Table 1**

Indicative Timeline	Events
31 December 2020	Commercial to invite shortlisted suppliers for this opportunity.
4-15 January 2021	Clarification period starts and closes
18 January 2021	Responses to CQs finalised and received by Commercial
19 January 2021	Respond to all outstanding CQs to suppliers
25 January 2021	Deadline for Supplier submission
18 January 2021	Commercial issue technical submission for evaluation team.
26 – 29 January 2021	Evaluation of proposals starts and completes
1 February 2021	Moderation session
3 February 2021	Final Evaluation completed
4 February 2021	Pricing finalised- Preferred Supplier Identified

5 February 2021	Successful and unsuccessful Suppliers notified
8 -12 February 2021	Final draft call -off contract received from supplier &Supplier set up (If supplier is new to MOJ)
12 February 2021	Contract Award (signed)
15 February 2021	Contract & Onboarding commencement
16 February 2021	Testing
22 February 2021	Live Service in place

9. Functional Requirements

The detailed requirements are listed below and have been assessed for their suitability and priority using the following criteria:

Conventions

Priorities have been assigned to requirements using the MoSCo convention as follows:
M = Must - Mandatory requirement
S = Should - Highly desirable requirement
C = Could - Desirable requirement

Further volumetric and statistical information can be found in the Non-Functional Specification.

Functionality Requirements Table 2
Case Management Application

No	Products	Requirements	M/S/C	Response Y/N/P	Civica Additional comments
FC1	Case	The case solution must be able to allocate a unique reference/case number/case type.	**M**	**Y**	**Auto allocation of reference provided as well as search by old reference were applicable**
FC2		The case solution must enable the Authority to create, edit, view, delete and override case details/notes/criteria	**M**	**Y**	**Subject to user access permissions users can create/edit/amend and delete case information. All changes made by users are recorded in the system audit trail.**
FC3		The case solution must provide the facility for Case Managers to be able to organise and manage cases for which they have responsibility.	**M**	**Y**	**Case Managers can view and organise their cases, including scheduling actions and reviews**
FC4		The case solution must provide an easy to navigate user interface, using language that will be familiar to OSPT staff.	**M**	**Y**	**The iCasework for Legal system provides an easy to navigate UI using similar descriptions to the current Prescient+ system.**
FC5		The case solution should be able to generate correspondence via email and print.	**M**	**Y**	**Both email and correspondence generation and printing is provided.**

FC6		The case solution must provide contextual help to users such as system and process functions. This help should be business configurable	**M**	**Y**	**In addition to on line help facilities, access is also provided to a library of Video Training/refresher modules**
FC7		The case solution must enable cases to be linked by reference number.	**M**	**Y**	**Cases can be linked, and can also have a parent/child relationship, or be sibling cases.**
FC8		The case solution must enable the upload of documents in various formats including any meta data associated with the document.	**M**	**Y**	**The system supports the upload and storage of most digital media formats, along with metadata**
FC9		The case solution should flag inbound communications from OSPT users	**S**	**Y**	**Confirmed**
FC10		The case solution should be able to recognise and automatically assign and update status according to events	**S**	**Y**	**Confirmed case status and updates to the status can automatically be linked to events or the completion of tasks.**
FW1	**Workflows**	The case solution must enable the Authority to manage its business process through a series of manual and automated steps. Referred to as workflows	**M**	**Y**	**Workflows can be implemented as part of the system, with workflows being customisable to meet specific requirements.**
FW2		The case solution must have the ability to escalate notifications	**M**	**Y**	**Escalations can be applied to both tasks and events**
FW3		The case solution must be able to create criteria-	**M**	**Y**	**Confirmed, events can be created via criteria**

		based events and event driven activities/tasks			**selection/application as well as tasks/activities**
FW4		The case solution must track and report on case progress or status	**M**	**Y**	**Case progression is tracked and viewable at case and team levels. Both Dashboards and reports can be provided to show case progression.**
FW5		The case solution should create case status notifications and warnings and inform users and customers when deadlines are due via an in-application dashboard.	**S**	**Y**	**Case Status and notifications are provided as part of the system, and the system provides user/team/department dashboards which inform users of key actions and status**
FW6		The case solution should give the user the ability to customise who receives notifications (internal and external), ideally with use of a prompt	**S**	**Y**	**Notifications can be customised**
FW7		The case solution should enable automatic allocation of activities/tasks to specific users and business groups	**S**	**Y**	**Activities/tasks can be allocated to both specific users, and user roles. E.g. Team Leaders.**
FR1	**Reporting**	The solution must have a built-in reporting tool which will enable end users to report on case data	**M**	**Y**	**The iCasework for Legal system is supplied with its own reporting tool, which provides for users with relevant access permissions to run amend and create reports using a wide range of criteria. Users can be given access to a library of**

					reports, which they can run on demand or access to the ability to build their own ad hoc reports as required. **Reports can be created in a variety of formats including pivot tables, charts and graphs, with interactive drill down into supporting layers of information and ultimately into cases/matters.** **The system provides for reports to be scheduled to run on an automatic basis e.g. daily, weekly etc., and reports can be automatically disturbed by email notification to recipients.** **Users can also be added to a subscription for a report, which will automatically send copies of reports to email recipient (both internal and external).**

					Reports can be also be output in a variety of formats. **In addition, support is provided for integration with MS PowerBI, with relevant users able to interrogate iCasework directly from within Power BI. In addition it is also possible to include Power Bi Dashboard/report views within the iCasework system using iframes within the system**
FR2		The reporting solution must enable the Authority to build, configure and store reports, with all available case data	**M**	**Y**	**Confirmed see above**
FR3		The reporting solution must provide standard and ad hoc reports in live and historical data at any time	**M**	**Y**	**Confirmed see above**
FS1	**Search**	The case solution must include an integrated search function which will enable the Authority to find and search records and data using a comprehensive variety of criteria.	**M**	**Y**	**Comprehensive search tools are provided which enable users to search records by multiple criteria.**
FS2		The search function must enable users to search using single or multiple fields	**M**	**Y**	**Confirmed**
FS3		The system must enable users to search for	**M**	**Y**	**The system supports searches against**

		electronic documents stored against a case record using existing metadata.			**document key words, user defined "tags" and a free text search of document content.**
FD1	**Data Management**	The solution must provide archive functionality for case records and enable the authority to comply with GDPR regulations	**M**	**Y**	**A case archive and user definable retention policy is provided to support compliance with GDPR**
FSE U1	**Security (End User)**	The case solution must enable the Authority to set, assign or remove appropriate user permission levels	**M**	**Y**	**Confirmed relevant users can determine user access levels.**
FSE U2		The case solution must allow passwords to be created and reset by the user within parameters set by the authority	**M**	**Y**	**Confirmed, either using Single Sign On, or the system controls. Please see attached Security whitepaper for details.**
FSE U3		The case solution must allow the Authority to set, assign or remove appropriate case access levels and apply the principle of least privilege for all data access. This means restrict by data content, and restrict to read-only rather than read-write wherever possible and appropriate	**M**	**Y**	**Confirmed,**
FSE U4		The case solution must ensure unique per-user accounts.	**M**	**Y**	**confirmed**
FA1	**Audit**	The case solution must log specific transactions including viewing and editing of data as defined by the Authority	**M**	**Y**	**A full transaction log is held including both viewing and editing of data.**

FA2		The case solution must date/time stamp all activities that occur	**M**	**Y**	**Confirmed all activities are data and time stamped**
FA3		The data management function must enable permitted users to access and view audit logs	**M**	**Y**	**Confirmed.**
FA4		The data management functions must provide the ability to archive historical data automatically according to the Authorities' criteria.	**M**	**Y**	**Confirmed. The system provides for use defined archive and retention policies.**
FA5		The data management functions must provide the ability to roll back user actions and changes for example a mistaken deletion of data	**M**	**Y**	**Confirmed**
FA6		logs and other auditable material must be stored remotely to ensure forensic diagnosis capability following incident	**M**	**Y**	**Confirmed**

Hosting and Infrastructure

No	Products	Requirements	M/S/C	Response Y/N/P
FHI1	**Hosting and Infrastructure**	The Case Management Solution must be hosted within Public Cloud in line with MoJ's requirements for OFFICIAL data (https://ministryofjustice.github.io/security-guidance/mythbusting/data-sovereignty/#data-sovereignty)	**M**	**Y**
FHI2		The hosting solution must comply with the Authority's Business Continuity Plan and in the event of disaster within the hosting environment that functionality and data can be recovered in under 8	**M**	**Y. Please see attached system security and architecture whitepaper attached**

		hours. (operational backups are covered in NFDR4)		**for details of the system BCP and system recovery times**
FHI3		The hosting solution must be able to be accredited to appropriate NCSC Security Guidance	**M**	**Y**
FHI4		The hosting environment must facilitate the capacity to support interfaces and data flows to and from integrated systems	**M**	**Y**
FHI5		The solution must be accessed by the OSPT customers, from the public Internet using web browsers via HTTPS. Browsers should be supported, E11 and FF68.1 and all modern browsers	**M**	**Y. The system provides a client portal, which enables customers to access case details, the level of information available being defined by the OSPT.**
FHI6		The hosting environment must: ● Support the anticipated performance load ● Provide antivirus software and services for the solution hosting environment. ● Provide sufficient storage capacity to manage the expected requirements ● Provide management information to enable the Authority to understand how its systems are being utilised	**M**	**Y** **The system iCasework application servers are implemented through AWS Elastic Beanstalk. Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. Elastic Beanstalk leverages AWS services such as Amazon Elastic Cloud Compute (Amazon EC2), Amazon Simple Storage Service**

				(Amazon S3), Amazon Simple Notification Service (Amazon SNS), Elastic Load Balancing, and Auto Scaling to deliver a highly reliable and scalable infrastructure. We utilise Elastic Beanstalk's inbuilt load-balancing features (scaling in additional servers on demand) as well as its cross region failover to ensure fault tolerance and automated system failure recovery. **Please see the attached security and system architecture whitepaper for further details.**
FHI7		The hosting solution must be able to deliver satisfactory response times on the existing / planned MoJ's network	**M**	**Y** **Please see the attached security and system architecture whitepaper for further details.**
FHI8		The solution must be capable of working with standard monitoring and systems management tools	**M**	**Y** **Please see the attached security and system architecture**

				whitepaper for further details.
FHI9		The application must have an availability level at the data centre of least 98.9% per year (Planned outages excepted)	**M**	**Y** **Please see Service Level agreement attached for details of system availability.**
FHI10		The hosting solution should offer a flexible processing and storage capacity – such that the Authority only bears charges for the capacity utilised and consumed	**S**	**Y**

Systems Integration

No	Products	Requirements	M/S/C	Response
FSYI1	**Systems Integration**	The supplier must ensure that all the components of the solution work seamlessly together to create an efficient and effective monitored end-to-end solution.	**M**	**Y**
FSYI2		The supplier must ensure that all elements of the solution will: Integrate with any enterprise based Active Directory structure to enable single sign-on). Integrate with MS standard Office tools. Integrate with the CAT? Integrate with a range of different published APIs?	**M**	**Y** **Integration with AD is provided to support SSO.** **Integration to MS Office and Office 365 is provided as standard.** **A system API is also provided to support integration with other third party applications and web services.**

Service Integration and Management (SIAM)

No	Products	Requirements	M/S/C	Response
FSIN 1	**Service Integration**	The supplier must document all aspects of Architectural Governance including implementation of a system of controls over the creation and monitoring of all architectural components and activities and ensuring compliance with the Authority's standards.	**M**	**Y.** **Please see Please see the attached security and system architecture whitepaper for further details.**
FSIN 2		The supplier must ensure that their Service Design Standards conform to the Cabinet Office Service Design and Delivery Guide.	**M**	**Y** **Please see the attached security and system architecture whitepaper for further details.**
FAS 1	**Application Support**	The supplier must supply 2nd and 3rd line application support (first line to be performed by MoJ Technology Service Desk)	**M**	**Y. Noted and confirmed**
FAS 2		The supplier must ensure application support is available to the Authority during working hours, as outlined under the relevant Service Level Agreement.	**M**	**Y** **Please see attached SLA**
FAS 3		The supplier must service levels and work with the authority to deliver improvements	**M**	**Y**
FAS 4		The supplier should create and maintain detailed and accurate end-to-end Service Level Agreement reporting and will use this data to provide management information to the Authority and to initiate service improvement actions.	**S**	**Y**
FET E1	**End to end Business**	The supplier must supply and maintain a comprehensive plan and service for:	**M**	**Y**

	Process Management	Incident Management Problem Management Event Management Continuity Management Availability Management Change Management Release Management Security Management		**Please see both SLA and system whitepaper attached.**

10. Non-Functional Requirements

The detailed requirements are listed below and have been assessed for their suitability and priority using the following criteria:

Conventions

Priorities have been assigned to requirements using the MoSCo convention as follows:
M = Must - Mandatory requirement
S = Should - Highly desirable requirement
C = Could - Desirable requirement
Non-Functional Requirements

Non- Functionality Requirements- Table 3

No	Products	Requirements	M/S/C	Response Y/N/P
NFI1	**Interoperability**	Integration with third-party applications or services must take place over open standards such as TCP/IP, HTTP, JSON/JSONP or XML. ?	**M**	**Y. Supported using system API**
NFI2		Interfaces with internal and external parties must comply with HMG standards.	**M**	**Y**
NFL1	**Legal and Regulatory**	The supplier must ensure that any solution (technical or business process) adheres to OSPT Legislation). For example, the solution must not be designed in such a way that it limits or allows certain practices or processes which impact the role of the OSPT	**M**	**Y**
NFL2		The solution must adhere to the Equalities Act and be able to support Assistive Technology Users.	**M**	**Y**
NFL3		The solution must adhere to General Data Protection Regulations (GDPR)	**M**	**Y**
NFH1	**Hours of Operation**	OSPT users typically work between the hours of 7am and 7pm, Mondays to Fridays but should be available outside of these hours		**Y The system is available 24/7 365**
NFH2		Some weekend working does take place within the sites but on a limited scale.		**Noted, support for the platform is available on a 24/7 365 basis**
NFA1	**Accessibility**	The solution must comply with the Disability and Equality Act.	**M**	**Confirmed**
NFCS 1	**Capacity and Scalability**	The solution must be capable of supporting 200 concurrent users consuming system resources at any one time. The solution must be scalable if the authority increases the number of users.	**M**	**The system is supplied as a SaaS service, and scales to support the subscribed number of users. We have**

					clients with over 5000 user of the system. **Civica understand from the RFQ that 150 users are initially required; however, we have provided costs based on 170 users to provide capacity for expansion/growth.**
	NFCS 2		The solution must be able to support an average of 120 new cases per day and be able to flex to support spikes in demand and other workload fluctuations.	**M**	**Y. The system is designed to auto scale to support fluctuating workloads.**
	NFAV 1	**Availability**	The application must have an availability level at the data centre of least 95% per year (Planned outages excepted)	**M**	**Y. The Service guarantee provides for a 99.5% availability level. Please see the Service Level agreement for full details of availability.**
	NFAV 2		The solution must provide business continuity in the event of a failure.	**M**	**Please see details within the SLA document.**
	NFS1	**Security**	The solution must adhere to HMG Security Policy Framework guidelines.	**M**	**Confirmed**
	NFS2		The solution supplier must define, document and agree with the Authority the roles and responsibilities of their staff and sub-contractors whom are responsible for administering and operating the solution.	**M**	**As part of the project, planning and governance process Civica agree and define with the client the roles of staff in**

					the administration of the system.
	NFS3		All staff and sub-contractors must be cleared to SC level.	**M**	**Y**
	NFS4		The solution supplier must ensure that all users and relevant employees have their solution access rights revoked on termination of employment.	**M**	**Y**
	NFS5		The solution supplier must ensure that all solution information and assets and supporting utilities are provided appropriate physical protection from internal, external and environment threats.	**M**	**Y. Please see security document attached.**
	NFS6		The solution supplier must ensure solution supporting utilities (hardware, firmware and software including hosting) are maintained and patched up to date, preventing loss or interruption of services.	**M**	**Y. provided as part of the SaaS provision.**
	NFS7		The solution supplier must define, document, agree with the Authority and regularly maintain (at least annually) Standard Operating Procedures for solution administration and maintenance, in line with the support and accreditation requirements.	**M**	**Noted and confirmed**
	NFS8		The solution supplier must ensure that their business continuity and disaster recovery arrangements conform to the Authority's business continuity plans.	**M**	**Noted and confirmed**

	NFS9		The supply must provide protective monitoring to support the detection of malicious activity. This should include: ● Network enterprise event monitoring ● Application management ● Hosting Enterprise Event Monitoring	**M**	**Please see the attached security document, which details the protective monitoring provided as part of the SaaS.**
	NFS10		The solution must provide controls that prevent log information from being modified.	**M**	**Application and system logs cannot be modified.**
	NFS11		The solution supplier must ensure their staff that are solution users have their access rights periodically reviewed and when a user role changes.	**M**	**Confirmed, staff access rights are reviewed on regular basis in line with their current role.**
	NFS12		The solution must suspend or shut down its sessions after a pre-defined period of inactivity	**M**	**Confirmed. User access sessions are closed after a pre-defined period. The length of time is controlled by client system administrators.**
	NFS13		The solution supplier must ensure that the solution is appropriately isolated from their other customer environments.	**M**	**iCasework on-demand services utilise Amazon RDS Aurora, which runs inside the iCasework Amazon Virtual Private Cloud in a separate AWS account for complete network isolation. Each customer's data**

					is held in a separate database schema to minimise security risks and to enable easy redeployment of customer data at any time. **Amazon RDS Aurora uses the industry standard AES-256 encryption algorithm to encrypt data stored in the database, as well as all automated backups, read replicas, and snapshots. Encryption keys are controlled by iCasework**
	NFS14		The solution software and firmware components must have full vendor support arrangements (security and general fixes).	**M**	**Confirmed**
	NFS15		The solution software and firmware components within the live, DR and NLE/Test environments must be patched up to date, in line with the patch management policy to prevent consumers from exploiting technical vulnerabilities	**M**	**Confirmed**
	NFS16		The solution must have any technical vulnerabilities identified from a penetration test treated (reduced, avoided, transferred or accepted) at intervals of not more than 12 calendar months since the last successful tests before any major change to infrastructure goes live, including but not limited to modifications to functional capability,	**M**	**As well as internal penetration testing the NCC Group have been commissioned to conduct annual external penetration tests as well as quarterly ASV scans to ITHC standards (UK data centre) and**

			implementation, or hosting any issues identified during Penetration tests or IT Health Check as a result of service changes must be mitigated or accepted before the service changes go live		**PCI DSS standards (Ireland, US and Australia data centres).**
	NFS17		The solution supplier must respond to incidents and report on incidents as specified within the incident management plan.	**M**	**please see SLA details**
	NFS18		The solution supplier must document, implement and regularly test and review business continuity arrangements for their facilities, utilities, and systems that support the solution.	**M**	**Our ISMS procedures include daily, weekly, monthly and quarterly routines to check logs and identify issues regarding security, scaling and systems administration. CloudWatch logs and metrics originating from multiple sources can easily be searched, analysed and correlated.**
	NFS19		The solution supplier should ensure that OSPT Protectively Marked information or personal information is not processed on development and test environments.	**S**	**Noted and it is our policy that no client data is used in test or development environments.**
	NFS20		The solution supplier should have an Information Security Policy that reflects the control objectives as specified within the ISO27001 control set.	**S**	**Y. Civica hold ISO27001 accreditation.**
	NFS21		The solution supplier should ensure that their development and test environments are appropriately separated from the live environment.	**S**	**Y, Noted. Test and development system are held in different data centres to ensure separation from live systems.**

	NFS22		The authority requires Cyber Essentials Plus (commonly 'CE+') certification and it is highly recommended that suppliers have NCSC Commercial Product Assurance (CPA) https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa for their products or services. If the tool chosen is cloud based, the authority would also be looking for alignment with NCSC Cloud Security Principles https://www.ncsc.gov.uk/collection/cloud-security	**M**	**The Civica iCasework team holds both PCI DSS and ISO 27001 certifications of its Information Security Management System (ISMS) covering provision of software, software hosting and software implementation services. Along with**
	NFS23		The solution must enforce Multi-factor authentication (MFA) access controls	**M**	**Y. iCasework authentication of caseworkers and separately customers can be configured to use single sign-on using either SAML/ADFS or Open Id Connect/oAuth.**
	NFS24		All data must be encrypted at rest and in transit.	**M**	**All iCasework on-demand services are delivered to end users using Transport Layer Security (TLS 1.2, 2048 bits) encryption ensuring all data input, REST api communications, file upload, data output and reporting facilities are encrypted at all times.**

	NFDO1	**Documentation**	Supplier should provide a High-Level and Low-Level Design documenting the proposed solution. This should include: Data Dictionary Reference to API Schemer Security Policy Service Level Agreements Training Guides Evidence of Accreditation	**S**	**As part of the implementation, process full details of the Data Dictionary and API Schemers will be provided. Details of our security policy and SLA are provided within the attachments to this response.**
	NFDE1	**Delivery**	The Solution delivery project manager must work with the team nominated by the Authority and report against agreed delivery milestones aligning with the overall project delivery plan and business change implementation plan.	**M**	**Y. Noted and agreed, as part of the implementation process the Civica project team will agree and document delivery milestone and the business change process.** **Please also see the Civica Legal implementation approach document included within the appendices.**
	NFDE2		The supplier is expected to provide project management and resources for the delivery of the solution	**M**	**Y. Civica have included within the services for the project, project management and implementation resources.**
	NFT1	**Training**	The Supplier must provide training and training courseware and system administrator guidance notes to users in training workshops, which can then be re-used by the Authority under a 'train the trainer' model	**M**	**y. A full set of training courseware will be provided along with access to video guides on the use of the application**

	NFM1	**Monitoring**	Data reporting must not affect performance of the production service.	**M**	**Y. The system platform is designed to scale to support user and application demands including reporting.**
	NFM2		The supplier must provide performance reports providing information on: • Business transaction volumes • Computational transaction volumes • User concurrency • End-to-end transaction times • Data centre boundary transaction times • Application availability • Breakdown of server availability • Capacity should be produced monthly	**M**	**Y. Noted. Civica would be happy to provide monthly performance reports on all of these areas.**
	NFR1	**Resilience**	The application must not have a single point of failure within the data centre. All application components within that data centre should be duplicated or have some form of failover	**M**	**Confirmed. Please see the attached AWS security paper, which provides details on security and data centre designs.**
	NFR2		In the event of an application component failover, the application must still be capable of supporting the defined peak load.	**M**	**Noted and the platform is design to support peak load at all times**
	NFR3		The application's disaster recovery facility must be equal to the application's live facility both in terms of access to the data and capacity.	**M**	**Confirmed. Please see the enclosed iCasework security and system architecture white paper for further details.**

	NFR4		The application backup must be tested at least once a year through a full backup restoration exercise. Details of the test and results to evidence success should be agreed with the authority	**M**	**Internal web security vulnerability assessments are performed on a quarterly basis or as a result of any new code releases or upgrades in the Web server software or operating system(s).** **Some areas of the testing cover input data validation for vulnerabilities** • **Audit our vulnerability to SQL Injection attacks on a quarterly basis.** • **Audit our vulnerability to Cross-Site Scripting attacks on a quarterly basis.** • **Check for broken authentication and session management vulnerabilities on a quarterly basis.** • **Check for insecure direct object references on a quarterly basis.** • **Audit our vulnerability to cross-site request forgery attacks on a quarterly basis**

					The outcome of the testing will be reported to the Information Security Manager. Any issues identified will be treated through the Security Event-Incident Responding Procedures (ISMS OP 06). **Independent external testing** **NCC Group have been commissioned to conduct annual external penetration tests as well as quarterly ASV scans to ITHC standards (UK data centre) and PCI DSS standards (Ireland, US and Australia data centres).**
	NFR5		In the event of the loss of a single data centre: ● The application should be online within 8 working hours. ● Data loss must be restricted to the last 30 minutes of transactional activity	**S**	**Amazon EC2, RDS and S3 provide data centres in a number of different regions (i.e. different physical locations) and feature automatic failover across these data centres.** **Should automatic failover fail, a completely new environment can be created with data recovered from an exact point in time**

					(last 35 days) typically within 30 min to 2.5 hours (depending on the time of day).
	NFLG 1	**Logging**	Log files must not be allowed to grow to the extent that they affect system performance.	**M**	**confirmed**
	NFLG 2		In the event of an error, the application log file should provide enough information for support teams to isolate the point and possible cause of failure.	**S**	**Every single action or update to a case is audited, providing a complete record of each stage in the process, with "actions" and "events" presented through a timeline view to deliver an instant visual display of a case's progression over time. Detailed activity logs on case data accessed and updates carried out are maintained at all times, logging who accessed what data at what time and from which network address. For update transactions, full details of the actual change made are logged. The system also stores any read access within the case audit trail.** **In addition to case related logs, the system also keeps a**

					record of administrative and configuration changes made by either customer or iCasework support staff. **Security incidents such as failed login attempts, attempts to access the system from an unauthorised IP address etc. are also stored in the iCasework audit trail.** **iCasework audit trail details cannot be deleted or amended. Audit trail data relating to cases is removed along with other case details in line with case retention periods configured**
	NFD R1	**Data Retention and Backup**	The solution must be incrementally and completely backed up at intervals appropriate to ensure business continuity.	**M**	**The automated backup feature of Amazon RDS Aurora also enables point-in-time recovery, allowing us to restore the database to any second during the 35 days, up to the last 5 minutes. AES256 encryption algorithms are used to encrypt all data stored at rest in the database, as well as all automated backups, read**

					replicas, and snapshots.
	NFD R2		The solution must be accompanied by a data restoration plan. This plan will encompass foreseen maintenance tasks such as replacing hardware, or rebuilding/modifying/replacing the operating system; as well as unforeseen events such as system failures or power outages.	**M**	**Confirmed a data restoration plan is provided**
	NFD R3		The application must hold data only for as long as is specified by the data retention schedule as specified by the Authority.	**M**	**Confirmed. Data retention schedules are defined by system administrators**
	NFD R4		All server volumes should be stored and replicated. The snapshot frequency should be applied to all volumes as follows: ● Every 2 hours with a 24-hour retention ● Nightly with a 7-day retention ● Weekly on a Sunday with a 2-week retention	**S**	**The automated backup feature of Amazon RDS Aurora also enables point-in-time recovery, allowing us to restore the database to any second during the 35 days, up to the last 5 minutes. AES256 encryption algorithms are used to encrypt all data stored at rest in the database, as well as all automated backups, read replicas, and snapshots.**
	NFD R5		The restoration of data should take no longer than 1 working day from the point of the request being made.	**S**	**The automated backup feature of Amazon RDS Aurora also enables point-in-time recovery, allowing us to restore the database to any second during the 35 days, up to the last 5 minutes. AES256**

					encryption algorithms are used to encrypt all data stored at rest in the database, as well as all automated backups, read replicas, and snapshots.
	NFD R6		Cached or 'past expiry' data must be purged as soon as possible, unless subject to a Retention Order, as specified by the authority.	**M**	**Confirmed, all data is purged automatically in line with the clients data retention policy**
	NFTE 1	**Testing**	The solution must provide a non-live environment which can be used for development and testing.	**M**	**Confirmed, a UAT system is provided for testing and development.**
	NFTE 2		The non-live environment must be updated and be an accurate representation of the live system in terms of patching and security processes.	**M**	**Y. The non live system is updated at the same time as the live system**
	NFTE 3		The supplier must provide and execute full testing.	**M**	**Confirmed, Civica provide and carry out full testing of software before release to UAT systems**
	NFTE 4		The supplier must provide and execute security tests that prove users can only access authorised data and functionality.	**M**	**Confirmed. Civica can provide details of the security testing process**
	NFTE 5		The supplier must support User Acceptance Testing	**M**	**Confirmed. A UAT system is provided**

	NFTE 6		The supplier must document all testing for audit and customer acceptance	**M**	**Confirmed, UAT and audit documentation is provided**
	NFSS 1	**System Support**	The solution must be accompanied by a support plan that describes the technical and managerial processes necessary to support the solution once operational.	**M**	**Please see the attached SLA document**
	NFSS 2		The support plan must include a description of the support personnel and their roles, as well as the processes to resolve problems arising within the solution boundaries, and escalation policies.	**M**	**Please see the attached SLA document**
	NFSS 3		The support plan must include service support hours and response times to calls.	**M**	**Please see the attached SLA document**
	NFSS 4		The support plan must include details of third-party maintenance service levels and agreements including any OWA's	**M**	**Please see the attached SLA document**
	NFE1	**Exit**	As far as possible, the supplier must provide upfront costs of exit at the conclusion of the contract.	**M**	**Outline details of exit arrangements are included within the SLA document attached. Civica would be happy to agree detailed costs for exit arrangements.**
	NFE2		The supplier must provide a documented method for data extraction at the conclusion of the contract and data deletion using an NCSC approved standards (https://ministryofjustice.github.io/security-guidance/#data-destruction)	**M**	**Outline details of exit arrangements are included within the SLA document attached. Civica would be happy to**

					agree detailed costs for exit arrangements

1. **Request for Information Table 4**

Questions	Suppliers response (Maximum 500 words)
Please tell us how the service offering meets the Functional and Non- Functional requirements identified above	Civica believe that the proposed iCasework for Legal service meets all of the functional and non-functional requirements detailed in the RFQ, and we have provided in the response above additional comments detailing how the requirements are meet for specific functions. The iCasework for Legal system builds on Civica's extensive experience of providing Legal case management systems, and replicates many of the facilities provided in our Prescient+ system whilst using new technologies to provide new features and functions. As well as providing the functions required to support the OSPT requirements detailed in the RFQ, additional facilities are provided to address the requirements of the OSPT to track and account for client monies and transactions, with transactions logs and audit of financial transactions differentiating between income and capital receipts and expenditure.
Please provide details of any previous deployments of your product to central government / local authorities or similar organisations?	Civica have extensive experience of deployments to central government and local authority legal services teams. Clients using iCasework include HMCTS, which has over 7,000 users of the system for various applications, and the Departmental Solicitors Office of Northern Ireland, which has 250 users of the system. Local authority teams range from 50-100 users.

<table>
<tr><td>Due to the OSPT support requirements of 7am-7pm, how would your support levels align with this?</td><td>The support portal for iCasework is available on a 24x7x365 basis for the logging of calls; and the system infrastructure is monitored and managed on a 24x7x365 basis. P1 (system down) calls are addressed on a 24x7x365 basis. With response and fix times detailed in the Service Level Agreement.

UK based application support staff are available for direct support calls between 8.30am and 5.30pm during normal working days. Additional coverage can be provided at additional cost if required.

Please see enclosed Service Level Agreement for further details.</td></tr>
<tr><td>The current system holds a large amount of data (1.7 Terrabytes) how will your platform manage this level of data?</td><td>Civica have clients using the iCasework system with over 7,000 users, and 5-10 Terabytes of data. Legal service teams in particular hold significant volumes of data because of the large number of documents and email held against cases.

The OSPT data set of 1.7TB is in the context of the systems we provide an average size and the iCasework platform is designed to scale to support both application and storage requirements.</td></tr>
<tr><td>Please provide details of your onboarding / delivery process including how you will meet the March 2021 timeline for project completion?</td><td>An overview of our implementation and on boarding approach is included within the appendices to this response.

Further discussion will be required before a final project timetable can be agreed, but we would anticipate the following high level timetable (based on the contract sign off in February 2021).

<table>
<tr><td>Date</td><td>Event/Task</td></tr>
<tr><td>15th Feb</td><td>Contract sign off</td></tr>
<tr><td>22-27 February 2021</td><td>Initial Project Kick Off meeting. Objective to introduce teams, agree timescales and</td></tr>
</table>
</td></tr>
</table>

	activities needed to achieve go live, and agree roles and responsibilities.
1-5 March	Initial On boarding meeting to agree technical configuration actions and tasks, and data extract process for data migration
8-13 March	Start of configuration workshops with operational team
15-27 March	Upload of data for data migration, and data import process for testing in UAT system
29 March to 2 April	Commencement of service for UAT testing Training of UAT Testers
Mid April	Completion of UAT Sign off
April	Commencement of Administration and Super User training. Commencement of Train the Trainer
May	Commencement of End User Training
May	Live data extraction and Migration
May	Go Live
May	Post go live review

Additional Civica Comments

We have noted our assumptions in respect of the contractual terms to be agreed between the parties within the Pricing Matrix which complements this response to RFP and our pricing is offered subject to those stated assumptions.

If we are selected as your supplier for this procurement, as part of the contractual discussions, we would expect to identify the relevant dependencies upon you in order for us to successfully deliver this project. These will include (but are not limited to):

- Making relevant staff available in a timely manner to support the achievement of the timescales that are agreed between us.

- Contributing to the data migration process by ensuring that data is cleansed wherever possible and that the quality of migrated data is subject to timely review.

We note that you require licensing for up to 200 users. Our Pricing Matrix prices the solution for up to 170 users by default, with an optional price for adding users in excess of this number.

Appendix Five
Training course outlines

Training

Civica UK provides a wide range of training support including:-

- System Administration and User Maintenance training
- Back office accounts training (Cashier)
- Super User training
- Train the Trainer training
- End-user training
- Workflow training
- On line training and how to videos

Trainers have an in-depth knowledge of the software and have a great deal of experience in training staff at all levels and ability, from trainees to senior managers. Importantly they understand the practical issues surrounding the use of the software in a working environment and provide support and guidance with change management best practices. Helping key project stakeholders achieve high levels of end user “buy-in” is as critical a task to our trainers as ensuring successful knowledge transfer. The courses always include documented practical exercises which must be completed at key stages within each course and knowledge transfer is validated through questioning and active learning techniques. These exercises serve as key stage tests and give delegates hands-on experience to ensure that each delegate is acquiring the knowledge they will need in order to use the system quickly and efficiently. Our trainers aim to empower confident and independent users and support through the change process is maintained post go live with excellent training and coaching services available if required. Many clients appoint internal trainers for their on-going requirements and Civica UK therefore provides structured ‘Train the Trainer’ courses targeted at supporting the key objectives of the project. One of the major benefits of this approach is that it ensures that clients become self-sufficient and are able to schedule refresher courses and/or courses for new employees without reference or reliance upon Civica UK to provide the service in the future.

Train the Trainer Programme

Civica UK's 'Train the Trainer' programme provides a detailed training course for internal training staff (duration 3 days).

- Session 1: Learning materials & knowledge transfer
- Session 2: Agenda – knowledge transfer
- Session 3: FAQ's and trainers development support

Detailed over the following pages is a list of the standard courses which are used as the basis for a customised training programme for a client.

Code	Course	Attendees
SA1	**Systems Administration** This day is spent with the key personnel within the organisation who will be involved in the administration of the system. The day will include housekeeping routines, creation of users, and maintenance of codes. OUTCOME: Delegates will have the ability to create new users, set up and maintain codes, coupled with the ability to take care of routine maintenance.	**Administration/ Super Users**
DATA1	**Configure and Review Test Conversion** The purpose of this day is to facilitate configuration of the test conversion so that it becomes a fully functional system which can be used for training and testing. It is important that details such as; fee earner rates, activity descriptions, etc. are readily available. Delegates will also be shown how to access the 'blank' system which will be used to create the codes for go-live, insert nominals, etc. OUTCOME: Delegates will have the ability to set up fee earner rates, activity descriptions, etc. against the test database so that the test database is configured to reflect the client environment for training and testing purposes.	**UAT staff. Course provided as part of UAT Testing.**

MMEU1	**iCasework for Legal End User** Fee earners and secretaries will be trained on how to use the ICasework for Legal system to perform their day-to-day document and correspondence activities; how to find, create, store and send documents, e-mails etc., and how to create documents from template/precedent banks to multiple parties on a matter, etc. OUTCOME: Delegates will have the ability to manage matters through the use of the ICasework for Legal document and e-mail management system, and document assembly tool. Delegates will be provided with the skills to search, create, edit, store and send documents and e-mails whilst being able to create documents and emails via the ICasework for Legal document template/precedent bank to one and/or multiple parties on a matter.	**End-Users** (Fee earners and Secretaries)
PPSU1	**ICasework for Legal Super User** The trainer will provide the super user and/or in-house trainer with a more detailed look at what aspects the fee earners and secretaries will be trained on, i.e. how to use the ICasework for Legal system to carry out their day-to-day work; how to search for and enquire upon clients, matters, parties, financial ledgers, perform time recording activities, request billing guides, and process accounts transactions OUTCOME: Delegates will have the ability to navigate ICasework for Legal, search and enquire upon; clients, matters, parties, and financial ledgers. Delegates will also be able	**Super Users** In-house Trainer

	to perform time recording activities, request billing guides, and process financial transactions. This knowledge will be transferred to the client so that the delegate will be proficient and capable of providing in-house training.	
MMSU1		
	Matter Management Super User The trainer will provide the super user and/or in-house trainer with a more detailed look at what aspects the fee earners and secretaries will be trained on, i.e. how to use the ICasework for Legal system to carry out their day-today document and correspondence activities; how to find, create, store and send documents, e-mails etc., and how to create documents from precedent/template banks to multiple parties on a matter, etc. OUTCOME: Delegates will have the ability to manage matters through the use of the ICasework for Legal document and e-mail management system, and document assembly tool. Delegates will be provided with the skills to search, create, edit, store and send documents and e-mails whilst being able to create documents and e-mails via the ICasework for Legal document template/precedent bank to one and/or multiple parties on a matter. This knowledge will be transferred to the client so that the delegate will be proficient and capable of providing inhouse training.	**Super Users** In-house Trainer
PPEU2	**Advanced - ICasework for Legal End-User** This course will build upon what has already been learned from the basic *ICasework for Legal End-User* course for fee earners and secretaries. This session is scheduled to run a few months after go-live, when the basics have bedded in and users wish explore ways in which to expand and improve their efficiency through their use of the ICasework for Legal software. OUTCOME: Delegates, having previously been taught the basics around ICasework for Legal and having had hands-on experience of the system during and after golive will have the opportunity to learn about some of the advanced features to improve productivity and efficiency.	**End-Users** (Fee earners and Secretaries)

CMSU1	**Case Management Super User Training** Provides end-user case management training to all super users, to include discussions around security access. OUTCOME: Delegates will have the ability to manage matters through the use of the ICasework for Legal workflow system. Delegates will also gain an understanding of the security aspects so that the system can be further enhanced to reflect the way in which the organisation is structured and the way in which cases are managed by department, team, etc. including escalation hierarchies.	**Case Management Super Users**
CMSU2	**Case Management Super User - Workflow Training** Discussion around the use of, and access to, the ICasework for Legal To-Do lists whilst also assisting in the creation of initial basic workflows. OUTCOME: Delegates will have the ability to use and configure the To-Do lists whilst also being able to create basic workflows.	**Case Management Super Users**
CMSU3	**Case Management Super User – Case Details Screens Training** This course trains super users on the creation and maintenance of the ICasework for Legal case details screens, whilst also assisting in the creation of new case details screens on the live system. OUTCOME: Delegates will have the ability to create, edit and maintain the ICasework for Legal case details screens whilst also being able to create new case details screens to	**Case Management Super Users**

	ensure that additional and relevant matter data is captured and presented to users as required with the added capability for the data to be output to documents and e-mails via the ICasework for Legal document assembly tool, and for the data to be reported upon.		

CMSU4	**Case Management Super User - Document Production Training.** This course assists in the creation of initial template/precedent documents and also includes some discussion on; document import; branch addresses; location of stored multi-branch documents, etc. OUTCOME: Delegates will have the ability to create initial template/precedent documents with some discussion around document import, branch addresses, multi-branch documents, etc. so that the system can be further tailored to the organisation's way of working.	**Case Management Super Users**
CMSU5	**Case Management Super User Refresher and Review Day** This course offers one day refresher training with super users on-site to review work carried out on customisation of the ICasework for Legal case management system. OUTCOME: Delegates will have an opportunity to review customisation work to ensure best-practice is followed and to ensure any future customisation is optimised.	**Case Management Super Users**
CMSU6	**Case Management Super User – Review and Sign Off Day** This course offers a one day review with super users onsite Civica UK to check through the completed system and discuss final preparations for; training, final amendments by Super users, and pre-go-live sign-off by Civica UK. OUTCOME: Delegates will have an opportunity to review the customisation work to ensure that the completed ICasework for Legal system reflects the requirements of the organisation, with some grace for final amendments ahead of go-live and Civica UK sign-off.	**Case Management Super Users**

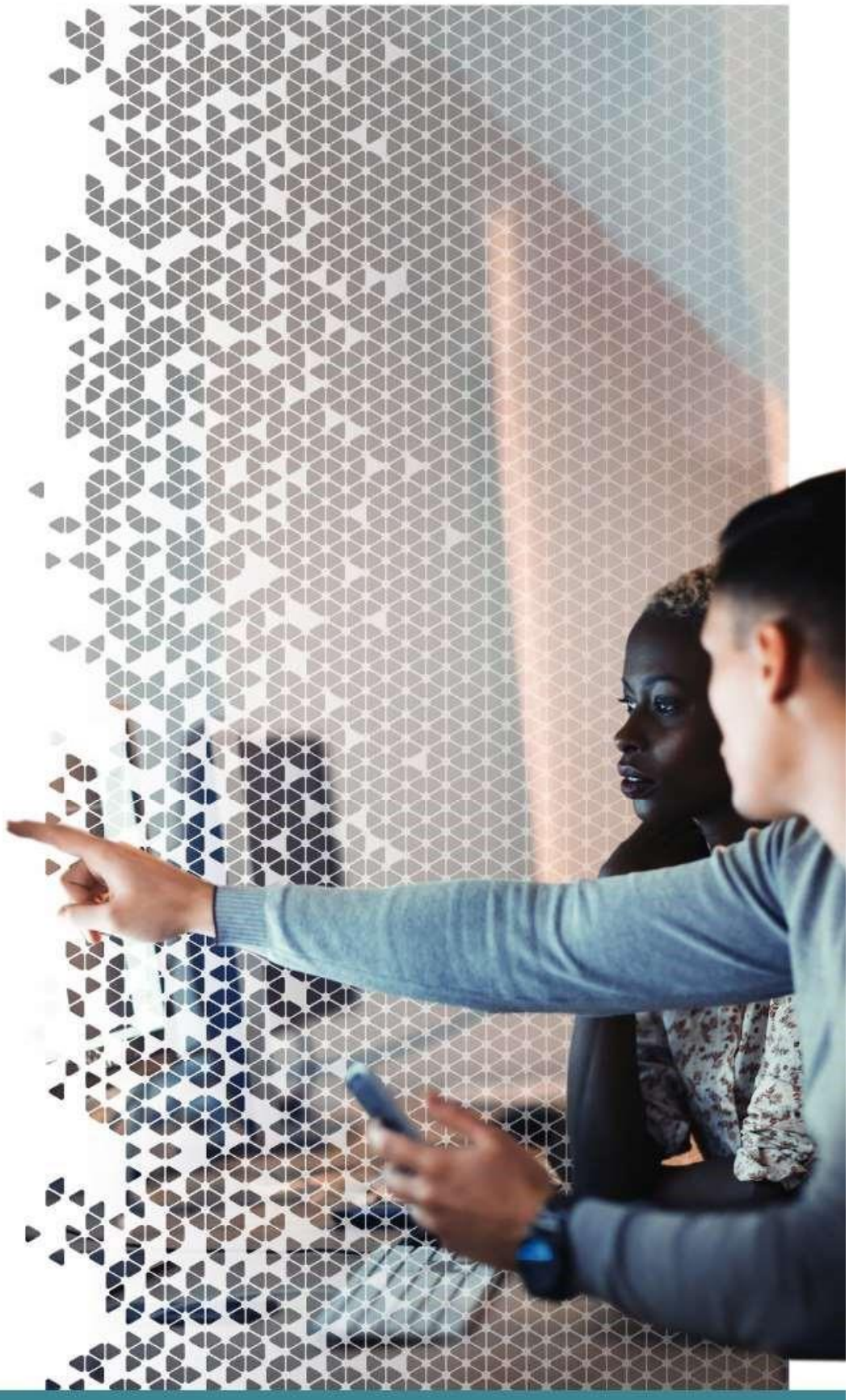
PMSA3	**Time and Charge Rate Administration** The super user group will trained in; the administration of time-sheets (once completed by fee earners on line), how to main-tain special charge rate structures, write-offs, and time trans-fers. OUTCOME: Delegates will be able to administer timesheets and maintain special charge rate structures, write-offs, and time transfers.	**Accounts Team**
BUND1	**Bundling System Implementation and Administration Day** To provide training for super users on the setup and administration of the ICasework for Legal Document & Court Bundling module OUTCOME: Delegates will have the ability to set up and carry out administration tasks on the ICasework for Legal Document & Court Bundling system.	**Case Management Super Users**
BUND2	**Bundling End User Training** To provide training for end-users on the use of the ICasework for Legal Document & Court Bundling module, ultimately to enable the creation of document and court bundles. OUTCOME: Delegates will be able to use the ICasework for Le-gal Document & Court Bundling system proficiently to gener-ate document and court bundles.	**End-Users** (Fee earners and Secretaries)

Appendix Six

iCasework Business Continuity Plan

civica

Transforming the way you work



ISMS 05 Business Continuity Plan

April 2020

V15

Document Owner:	
Name:	Business Unit (BU):
Compliance Manager	iCasework

Approved Author(s) / Editor(s):	
Name/Group:	Business Unit (BU):
Operations Director	iCasework
AWS Infrastructure Manager	iCasework

Approved Distribution:	
Name/Group:	Business Unit (BU):
iCasework Business Unit	iCasework

Commercial in Confidence

Contents

1. Introduction

1.1 Purpose and Scope

This plan has been developed so that the iCasework Business Unit (BU) within Civica Digital is prepared for any major interruption in its business operation or any disruptive incident.

The purpose of the Business Continuity Plan and associated procedures is to enable the iCasework Business Unit (BU) to respond to any interruption to the service or disruptive incident in a calm, structured and professional manner and to respond to the incident, resume and recover activities and services to an acceptable level and ultimately meet the requirements and goals as detailed in the Civica Business Continuity Management Policy.

1.2 Authority of this Plan

The plan carries the full authority of the iCasework BU Managing Director (MD) and Senior Leadership Team (SLT). The plan will be reviewed annually by the SLT for relevance and applicability.

1.3 Objectives

The objectives of the iCasework BU Business Continuity Plan are to:

- Identify and act immediately to possible interruptions or disruptions caused by internal and external events.
- Specify how the BU will react to these possible events.
- Ensure health and safety of employees, contractors, visitors who are within Civica's premises at the time of a disruptive event.
- Demonstrate an organised, unified response and that the situation is under control.
- Provide information that is accurate and factual and how the BU dealt with the disruption.
- Reassure and respond to the needs to customers, employees, business partners and other party as required.

1.4 Scope of disruption (disasters and failures) covered by this plan

The crises / failures covered by this plan are:

- Inability to access essential Information Communication Technology (ICT) infrastructure.
- Unavailability or restricted access to premises and facilities.
- Loss or illness of key employees or absence of significant number of employees.
- Outbreak of disease or infection (e.g. pandemic).

1.5 Activation of this Plan

The plan will be activated by the iCasework BU Managing Director or anyone from the SLT following discussions with the Managing Director. If possible, an email or text message will be sent to all iCasework BU employees and customers advising them of the activation. The iCasework support portal will have a message posted on it detailing the situation, if appropriate.

2. Context

2.1 Introduction

We design case management systems and provide hosting and support services for a wide variety of customers. This plan seeks to identify what the possible interruptions we may be faced with and how we can prepare for and deal with such interruptions and disasters.

2.2 Disaster and Failure Scenarios

The main disaster and failure scenario areas that were considered when identifying the business requirements for recovery and the related business continuity strategy for us is identified in the following sub-sections.

2.2.1 Unable to access the ICT infrastructure

Civica Internal Network (ICT Infrastructure)

The internal network comprise of a range of components such as file server, hub, router, switches, and associated cabling and could fail or be damaged or destroyed. In addition, PCs and Laptops could also fail or be destroyed.

Civica Shared Drive

The Civica shared drive provides a document storing service for management of various documents that are used in the BU. The shared drive could fail/be unavailable due to a failure/disaster on the Civica internal network.

ICT Applications / Email

One or more of the general applications such as Windows, MS Office (Word, Excel) and /or Email could become unavailable or fail.

IT Bespoke Applications

The only bespoke application is the Support System, which could become unavailable or fail.

Amazon Hosted Applications and Databases (AWS Infrastructure)

Our architecture consumes standard Amazon AWS's managed platform services or components such as Amazon Elastic Cloud Compute (Amazon EC2), Elastic Beanstalk (application service) and RDS Aurora (Amazon Relational Database Service), S3 (file storage service), SES (email service) and SNS (Simple Notification Service), which are resilient and hardened to security best practices.

Elastic Beanstalk, which is one of the key components in our Virtual Private Cloud (AWS VPC) manages the application servers as it automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. Amazon RDS Aurora manages the database instance on our behalf by performing backups, handling failover, and maintaining the database software.

Amazon EC2, RDS and S3 provide data centres in a number of different regions (i.e. different physical locations) and feature automatic failover across these data centres.

Should automatic failover fail, a completely new environment can be created with data recovered from an exact point in time (last 35 days) typically within 30 min to 2.5 hours (depending on the time of day). The Amazon cloud service could fail/be unavailable due to:

- a failure/disaster at Amazon's premises or over the link between Amazon's cloud services and our customers,
- a breakdown of the Amazon contract.

We have reviewed Amazon's business continuity plan, and is satisfied that it is complete and usable, and that it is commensurate with our business needs. However, even with a good plan in place and tested, the availability of the Amazon's cloud service cannot be taken as being guaranteed, and thus this must be taken into account in determining the business continuity strategy. Further, the efficient use of the Amazon cloud service depends on the continued availability of the Amazon cloud service.

We are an ISO 27001 accredited organization. A significant element of that accreditation process is demonstrating to external auditors that we have competent business protection and continuity in place. Our ISMS Framework provides evidence-based records of business continuity testing.

Backup of Cloud based services and databases

Cloud based services are backed up to a secure location with access restrictions. Other services and data are backed up and stored in different locations and on cloud-based platforms. The backup could fail due to:

- a failure/disaster during the backup or at the site where the backup data is stored,
- a breakdown of the arrangements between the Civica iCasework BU and Amazon.

Voice/Tele Communications

We are reliant on Skype for Business for our voice communications (internal and external) and this could fail.

2.2.3 Unavailability or restricted access to premises and facilities,

Utility Failure

We are dependent on water and electricity. If any of these fail because of problems, then the affected buildings could have to close (e.g. if there was no water a building may have to close on health grounds). In this circumstance, it is likely (although not guaranteed) that temporary access would be possible to retrieve equipment and documentation.

Related to this utility failure scenario, the consequent effects could be lack of lighting, heating, and a usable physical access security system, thus rendering the building(s) unusable (although probably accessible temporarily).

Building Loss

Unavailability/loss of part or one or more buildings can occur through environmental incidents such as fire, water damage, explosion etc.

Building Access Restrictions

Normal access to buildings may be denied or restricted through a range of factors including the utility failure scenario, civil unrest in the area, police cordons from terrorist incidents, building occupation and global pandemic. Access to the office may be:

- temporarily accessible but not usable,
- not accessible at all.

2.2.6 Loss or illness of key employees

Unavailability of employees

Employees may be unavailable for several reasons, including:

- significant loss of life (e.g. through fire, explosion),
- widespread failure of public transport through a major incident or industrial action,
- adverse weather conditions,
- widespread illness (e.g. disease, infection, an influenza epidemic, global pandemic)
- mass resignation or other form of industrial action.

Loss of critical employees

The loss of critical employees can have a major operational impact on a business. Considering the problem ahead of time allows the business to ensure that critical posts have pools of experienced and capable people to fill those posts in an emergency.

2.3 Key Business Priorities

We need to be able to:

- manage hour-by-hour the systems that Amazon are hosting for us (i.e. to provide support);
- access software to develop new software for customers;
- access software to amend existing software for customers;
- backup on an ad-hoc manner various databases and applications; access customer sites to undertake problem analysis; Contact customers and suppliers via email or telephone.

2.4 Summary of Business Requirements

The main provision here is to ensure that the iCasework BU have access to telecommunications, and computing technology including the internet, sufficient for them to field support calls and to fix short and medium-term problems for customers.

3. Overall Strategy

The overall strategy is to have in place, at short notice, the essential employees that can use their company issued laptops to access services. The aim is to minimise the impact of any interruptions by ensuring that the appropriate employees and equipment is available to respond quickly and effectively to such interruptions.

The following sections detail what disasters might occur to our business, requirements and agreements.

Area No.	Sub Area	Requirement	Agreement
3.1.1	Civica Internal Network (ICT Infrastructure)	The company can deliver services even if the main office is out of commission. Essential employees can deliver the required services as long as they have access to the Internet.	Ensure that essential employees have laptops with access to the Internet.
3.1.2	Civica Shared Drive / Access to Information Stored Electronically	We store all documents (both work-in-progress and completed) electronically. All such documents are retained on the shared drive which is backed up.	All documents must be stored on the shared drive, which is backed up. If there is a disc failure, then the last backup must be used to restore the data (if required). Hard copies of key documents, such as key operational records are stored in a secure cupboard at the registered office.
3.1.3	ICT General Applications / Email	We use MS Office and MS Outlook for emails.	Key contacts with our customers and suppliers will be maintained on a paper file.
3.1.4	IT Bespoke Applications iCasework Support Service Help Desk	The company needs to be able to respond, according to contract agreed timescales, to calls or reports from customers to our Support Desk.	If the system supporting the service fails, then it must be restored to a condition that allows it to be used. The website needs to have a message published on it advising of any down time for the support system, and what alternative arrangements are in place to keep up contact with customers.

Area No.	Sub Area	Requirement	Agreement
		The support team can be reached by phone in the UK on Monday to Friday 9am to 5.30pm (BST, excluding UK Bank Holidays) or by email. However, we especially encourage our clients to contact us via our Support Portal as this is accessible 24 hours a day, seven days a week.	
3.1.5	Amazon Hosted Applications and Databases (AWS Infrastructure)	We host on-demand services for its customers through Amazon Web Services (AWS). The requirement is that we can provide alternative arrangements in the event of a loss of an entire AWS data centre.	The Amazon services used are Amazon Elastic Compute Cloud (EC2), Amazon Relational Database Service (RDS) and Amazon Simple Storage Service (S3) are configured to utilize multiple data centers in a number of different regions (i.e. different physical locations) and these services feature automatic failover across these data centers. However, even if automatic failover should fail, a completely new environment can be created with data recovered from the RDS at an exact point in time (last 35 days) typically within 30 min to 2.5 hours (depending on the time of day). The infrastructure team members will follow the below procedure to bring the service backup. • Create a new running service using AWS Elastic Beanstalk Storage (EBS) in a working region using the last used war file; and • Use RDS to create the database to the exact point in time as necessary; and use Route 53 to map the customer's domain address to the domain address

Area No.	Sub Area	Requirement	Agreement
3.1.6	Backup of Cloud based services and databases	All company confidential data is backed up and is stored in a secure location and on cloud-based platforms, based on the required data we can access the cloud-based backups.	Our RPO and RTO is as follows: Recovery Point Objective (RPO): iCasework ondemand utilise Amazon RDS Aurora. The automated backup feature of Amazon RDS enables point-in-time recovery, allowing us to restore the database to any second during the 35 days, up to the last 5 minutes. Amazon RDS also features automated fail-over of the database to an alternative data centre (but within the same geographical zone) should this be necessary. Recovery Time Objective (RTO): Replica environments exist and are automatically failed over to in alternative data centres. Should failover fail, a completely new environment can be created with data recovered from an exact point in time (last 35 days) typically within 30 min to 2.5 hours (depending on the time of day).
3.1.7	Voice Communications	We have published telephone numbers for the support desk and the general office. A high number of calls from prospective customers are received on this general office number, and some support issues also need to be discussed over the phone. iCasework would like to have in place alternative numbers available in the event of landline difficulties. Much of the day-to-day contact with customers and suppliers is undertaken by the Skype for Business service and use of mobile phone if required. iCasework wants to continue such communication if this service is lost.	All customers and suppliers must be given a list of employees who can be contacted by mobile phone. In the event of a problem with the landlines, iCasework should publish a notification on the website alerting suppliers and customers of the new arrangements. Employees should have access to mobile phones in addition to the Skype for Business service.

Area No.	Sub Area	Requirement	Agreement
3.1.8	Unavailability or restricted access to premises and facilities	The company can deliver services even if the main office is out of commission. Essential employees can deliver the required services as long as they have access to the Internet.	Ensure that essential employees have laptops with access to the Internet, via the Civica VPN.
3.1.9	Loss or illness of key employee or absence of significant number of employees (outbreak of disease or infection (e.g. pandemic) Employee Shortages	The company needs to be able to provide support to services on a continuous basis from 9 to 17:30 on weekdays, and for backups and other system work on a 24/7 basis.	All support work is undertaken on a shared basis so that no individual team member is the only custodian of intellectual information about a service or system activity. If new services/technical activities are undertaken, then these need to be documented and shared with at least one other member of the team. If a key member of the team is absent, then the work load of other team members need to be re-calibrated to ensure that the impact of the missing team member is mitigated. If the employee shortage is more than just a shortterm activity, then the business must recruit to replace the absent employee(s).
3.1.10	Loss or illness of key employee or absence of significant number of employees (outbreak of disease or infection (e.g. pandemic) Transport Failure	Having essential employees at particular locations is not a requirement for us. However, if essential employees are stuck in-transit then we would expect to establish contact via mobile phone, and if necessary, take instructions from them.	Maintain a list of updated mobile and landline telephone numbers. Ensure that all essential employees, as a matter of course, carry their mobile phones. Provide access to copies of essential system documentation as a backup to the main store for such information.

3.1.11	Loss or illness of key member to the team or absence of significant	Succession Planning is the process by which a business can ensure continuity.	To follow through the Succession Action Plan as laid out in the Succession Action Plan Policy.
Area No.	Sub Area	Requirement	Agreement
	number of employees (outbreak of disease or infection (e.g. pandemic) Loss of critical employ-ees		

The principal implication of the plan is that arrangements must be put in place that will mitigate major interruptions. Employees must be aware of the existence of this Business Continuity plan and what is expected from them in the event that the plan is put in operation. We can cope with loss of access to offices and other physical impacts but is very reliant on the Internet and ICT arrangements. The mitigation efforts listed in the plan, if implemented, should reduce the impact of major interruptions

4. Organisation

4.1 Introduction

The iCasework BU organisation section of the plan will show who will undertake specific tasks to ensure that the company responds to a serious interruption to services. 4.2 Business Continuity / Recovery Organisation iCasework BU Organisational Structure

The Outward Facing Services of the BU and the persons/area responsible for them are:

External Service	Person/Area Responsible
Web Based Services	AWS Infrastructure Manager
Company Website	Civica Marketing
Server Centre's	Third Party (Amazon Web Services)

The Inward Facing Services of the BU and the persons responsible for them are:

Internal Service	Person Responsible
Finance and HR	Civica Finance and HR
AWS Architecture	AWS Infrastructure Manager
Internal Network:	Civica Group IT
Marketing	Civica Marketing
Development Centre	Product Director
Operations and Project Management	Operations Director

5. Logistics

5.1 Centre of Operation

The company can deliver services even if the main office is out of commission. Essential employees can deliver the required services as long as they have access to the Internet.

5.2 Management of Key Post Holder and Contact Details

Internal Service	Person Responsible
Web Based Services	Redacted
Company Website	Redacted
Finance and HR	Redacted
Internal Network	Redacted
Marketing	Redacted
Development Centre	Redacted
Operations and Project Management	Redacted

Communications

Ongoing communications throughout all Incident Management Phases (pre, during and following a disruptive incident) is of paramount importance to ensure all stakeholders are kept fully informed of the situation.

Following a disaster, the immediate business service priorities are

1. Business Unit Website, customer Portal,
2. Web Based Services,
3. Internal Network,
4. Development Centre

The priority order of contact relevant stakeholders is:

1. Contact all iCasework employees
2. Contact clients
3. Contact Amazon Web Services
4. Telephone numbers re-routed
5. Set up temporary office
6. Purchase Server(s) or access cloud-based services (as required)
7. Restore backups
8. Gain access (VPN or via cloud-based applications)
9. Update website

5.3 Public Relations

The Managing Director is responsible for any public relations issues. Depending on the circumstances, it may be considered appropriate to retain a professional PR function.

5.4 Transport Arrangements

We use electronic communications. Access to physical servers is not required. If there are any transport arrangements required these can be made at the time of the disaster.

5.5 Expenditure Control / Emergency Purchasing

This is managed by Civica Finance.

5.6 Remuneration / Personnel Policies in a Disaster or Failure

This is managed by Civica Finance.

6. Key Documentation and Operational Records

Key personnel, financial and legal documents are kept at the registered office and soft copies are kept in the internal company network.

All system documentation and operational records are maintained in an electronic format on computer systems, which are regularly backed up. Hard copies of key documents, such as key operational records are stored in a secure cupboard at the registered office.

In the event of a disaster these backups can be used to rebuild the store of electronic documentation.

7. Maintenance and Testing of the Plan

The plan will be reviewed every 12 months. The current version has been tested and the effectiveness of the plan needs to be tested every 12 months. All employees need to be aware of the plan and their role in it. Employees are encouraged to suggest amendments to the plan as they see fit. Such suggestions need to be considered by the Managing Director and the Operations Director.

The plan will be reviewed every 12 months. Any amendments will be tested and published If necessary, training will be provided if the plan is altered substantially.

The plan has been tested in terms of ensuring that the critical issues have been tested. These are checking the quality of backups (which is undertaken at any rate in the normal operational work).

The strategy is to ensure that the plan operates effectively and as specified.

Tests should be planned in advance.

Appropriate resources must be set aside for undertaking the tests.

8. Emergency Response

This plan is based on a major incident such as the destruction of the building. It can be easily adapted for less severe situations:

8.1 Alert, escalation and plan invocation

There are several different possible disasters, each of which may require partial or complete invocation of the BCP. We have a standard, rehearsed alert, escalation and BCP invocation procedure. The procedure is invoked by the Managing Director and/or Operations Directors when an incident requires the BCP to be put into operation.

Where the premises need to be evacuated, employees are must at the evacuation assembly point.

The Managing Director (or the most senior member available), must inform the Emergency Response Team (ERT) that a critical business system is unavailable, if either an identified problem has not been fixed / alternative arrangements made within two hours of notification of the problem or if the problem is unlikely to be corrected within two hours of its failure. The ERT will then decide the extent to which the BCP must be invoked.

8.2 Emergency Response Team (ERT)

The responsibilities of the ERT are to:

- respond immediately to a potential disaster and call emergency services,
- assess the extent of the disaster and its impact on the business,
- decide which elements of the Business Continuity Plan should be invoked,
- establish and manage a Service Continuity Team to maintain vital services,
- establish and manage a Disaster Recovery Team to return to normal operation,
- ensure employees are notified and allocate responsibilities and activities as required.

8.3 ERT Assembly Location

In the event of a disaster, the members of the ERT will attempt to contact each other and agree an assembly location for the ERT. In the absence of any other communication, members of the ERT will make their way in the first instance to the assembly point:

Any employees in the office at the time of the disaster, should report to these locations. Those who are not will be contacted.

8.4 ERT Action

The members of the ERT will take on roles and delegate activities to other team members according to the situation. The ERT will set clear objectives, defining responsibilities and priorities, and provide decisive leadership in dealing with business continuity issues.

The exact action to be taken will depend upon the circumstances; an ERT Action Checklist is at Appendix A of this section.

The members are the iCasework ERT team is the Operations Director and the AWS Infrastructure Manager.

8.5 Disaster Recovery Team

The composition of the team will be decided by the ERT depending upon the nature of the emergency. The responsibilities of the team are to:

- establish facilities for an emergency level of service within 6 business hours,
- restore key services within two days of the disaster,
- recover to business as usual within five days of the disaster,
- coordinate activities with the Service Continuity Team, report to the Emergency Response Team.

8.6 Service Continuity Team

The composition of the team will be decided by the ERT depending upon the nature of the emergency. The responsibilities of the team are to:

- ensure that key services continue with a minimum of disruption,

- agree the resource requirements with the Disaster Recovery Team, coordinate activities with the Service Managers,
- report to the Emergency Response Team.

8.7 Post Disaster Actions (Incident Report Form)

All details of the incident, along with decisions and actions taken are recorded on the Incident Report form. This report must be detailed enough to accurately describe what happened so that all who need to know can assess the quality of the plan and the actions taken when the incident occurred so that lesson learned can be captured and incorporated.

9. Appendix A Disaster Action Checklist

EMERGENCY RESPONSE TEAM DISASTER ACTION CHECKLIST

This action checklist is designed for emergency situations; there are several circumstances in which appropriate action does not require the full response.

Evacuation and calling of emergency services;

Calling Tree - starting and managing the calling tree mechanism: maintaining a handwritten log of the calls made, responses and agreed next steps;

ERT Office - setting up the ERT office with team members and facilities;

Call Logging - setting up and managing a mechanism to ensure that all incoming calls are logged, issues dealt with and calls returned as necessary;

Events - monitoring and logging events - information from team members, emergency services, and others;

Employees - determining the whereabouts and condition of employees- use of the checklist (Appendix E); dealing with immediate first aid and other needs; setting up trauma counselling if required; informing next of kin;

Facilities - buildings, furniture, equipment - assessing damage; determining immediate and longer-term needs; obtaining supplies; dealing with insurers and loss adjusters;

ICT, Web Based Service - determining extent of damage; setting up interim systems; planning recovery of full systems; restoring data from secure backup; recovering documents from off-site;

Service Continuity - invoke plans for business unit services; set up disaster information line for clients; decide which other services can be kept going and to what degree; ensure services continue according to plan;

Media - controlling and informing;

Finance - controlling the finances of the Business Unit ensuring that there is sufficient accessible finance for the BU to manage its business.

Salvage - obtaining help with recovery.

10. Appendix B Key Post Holders

Specific responsibilities related to the disaster will be allocated by the Emergency Response Team as required; it is likely to include the following:

- ICT / Web Based Service
- Premises
- Employees
- Media
- Finance

Alternates

Each team member has an alternate nominated person who has the knowledge and ability to be able to deputise, at least on a temporary basis, should that team member be unavailable.

Role	Holder	Alternate
Web Based Services	Redacted	Redacted
Company Website	Redacted	Redacted
Finance and HR	Redacted	Redacted
Internal Network	Redacted	Redacted

Marketing	Redacted	Redacted
Operations and Project Management	Redacted	Redacted

11. Appendix C Personnel Contact Numbers

IN CONFIDENCE - EMERGENCY USE ONLY

Personnel contact numbers

Name	Mobile	Email
Redacted	Redacted	Redacted

12. Appendix D Supplier Lists

All details on Amazon Web Services can be found on the internet. .

13. Appendix E Business Continuity Forms

Employee Call Checklist

1 Information

- Caller's name.
- Their whereabouts and a contact number.
- Their state of health.
- What they observed at the site of the disaster.
- Who else was known to be at the site - other members of the team or visitors Knowledge of other members of the team, who is safe, who is injured.
- Who they have spoken to e.g. police or press, and what they have said.
- Any practical difficulties e.g. lack of cash, lost home keys etc.

2 Assessment

 Determine how useful the person is likely to be in the immediate future, what roles they could take on, and whether there are likely to be other needs such as trauma counselling.

3 Instructions

Tell the member of the team:

- the location to which they should report, or to go home.
- their responsibilities during disaster recovery e.g.
- to attempt to continue their normal activities, to take on a specific responsibility, or to do nothing until otherwise advised.

- when to call again.

14. Appendix F Incident Report Form

The form below is to be filled in after an incident. It details what information should be included in a report to customers if they have been affected by an incident.

Service Disruption Dates / Times	Date Start dd/mm/yy Time Start hh.mm Date End dd/mm/yy Time End hh.mm
Introduction The report here should specify (and amend as appropriate): This report provides findings concerning a major disruption of services that occurred between dd/mm/yy and dd/mm/yy. Its purpose is to provide our customers with a general understanding of what caused the disruption, specific impacts and a chronology of events, the root cause of the disruption and the specific steps currently being taken to avoid future occurrences. We are acutely aware of the impact of loss of services. We regret the disruption and appreciate the patience of the customers as we worked through the underlying problems.	
Overview of the incident Specify here in overall terms what happened.	
Specific Impacts State here what were the specific impacts of the incident	
Root Cause Specify here the reasons why the incident occurred.	
Chronology Specify here the timeline of the events that transpired.	
Corrective and/or Preventative Actions In this section list in detail the actions required to correct the incident and any new actions that may be required in the future to deal with a similar incident.	
Conclusion Specify here all appropriate conclusions following from the incident, including lesson learned. If a review is required of planned responses, put it here. If it is already clear what extra actions are required, then specify them here. Be honest about the effectiveness of the plans and the actual response. Finally, if thanks are appropriate, then here is where it should be put.	

Document Control:				
Version:	Author:	Date:	Comments:	Status:
V14	iCasework	March 2019	iCasework Version	Publish
V15	iCasework	April 2020	iCasework Version updated to use Civica template.	Publish