



# Crown Commercial Service

L

## G-Cloud 12 Call-Off Contract

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

|   |    |
|---|----|
| Part A: Order Form.....                       | 2  |
| Schedule 1: Services .....                    | 12 |
| Schedule 2: Call-Off Contract charges .....   | 12 |
| Part B: Terms and conditions .....            | 13 |
| Schedule 3: NOT USED.....                     | 32 |
| Schedule 4: NOT USED.....                     | 44 |
| Schedule 5: NOT USED.....                     | 49 |
| Schedule 6: Glossary and interpretations..... | 57 |
| Schedule 7: GDPR Information .....            | 68 |

## 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.

|  |   |
|--|---|
| <b>Digital Marketplace service ID number</b> | 223535119855030   |
| <b>Call-Off Contract reference</b>           | CQC NGO 003   |
| <b>Call-Off Contract title</b>               | Case Management System – National Guardian's Office   |
| <b>Call-Off Contract description</b>         | To provide a case management system for initially 24 months with an option to extend for up to a further 24 months at 12-month intervals. |
| <b>Start date</b>                            | 01/12/2021  |
| <b>Expiry date</b>                           | 30/11/2023  |
| <b>Call-Off Contract value</b>               | £72,592   |
| <b>Charging method</b>                       | Annually for Subscriptions, Monthly for in arrears for other services.  |
| <b>Purchase order number</b>                 | TBC   |

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.

|                               |   |
|-------------------------------|---|
| <b>From the Buyer</b>         | Care Quality Commission<br>Buyer's phone: 0207 448 9086<br>Buyer's main address:<br>Citygate, Gallowgate, Newcastle upon Tyne NE1 4PA                   |
| <b>To the Supplier</b>        | IIZUKA Software Technologies<br>0121 200 8906<br>Supplier's address:<br>2 Church Court<br>Cox Street<br>Birmingham<br>B3 1RD<br>Company number: 4498601 |
| <b>Together the 'Parties'</b> |   |

### Principal contact details

#### For the Buyer:

Title: Business Manager

Name: [REDACTED]

Email: [REDACTED]@cqc.org.uk

Phone: [REDACTED]

#### For the Supplier:

Title: Greg Hayes Managing Director

Name: [REDACTED] Managing Director

Email: [REDACTED]iizuka.co.uk

Phone: [REDACTED]

### Call-Off Contract term

|                   |   |
|-------------------|---|
| <b>Start date</b> | This Call-Off Contract Starts on 01/12/2021 and is valid for 24 months. |
|-------------------|---|

|                                    |  |
|------------------------------------|--|
|                                    | <p>The date and number of days or months is subject to clause 1.2 in Part B below.</p>   |
| <p><b>Ending (termination)</b></p> | <p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least <b>90</b> Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of <b>30</b> days from the date of written notice for Ending without cause (as per clause 18.1).</p>  |
| <p><b>Extension period</b></p>     | <p>This Call-off Contract can be extended by the Buyer for <b>2</b> period(s) of up to 12 months each, by giving the Supplier <b>30 days</b> written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.</p> <p>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.</p> <p>The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.</p> <p>If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:</p> <p><a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a></p> |

## 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.

|                                  |   |
|----------------------------------|---|
| <b>G-Cloud lot</b>               | <p>This Call-Off Contract is for the provision of Services under:</p> <ul style="list-style-type: none"> <li>• Lot 2: Cloud software</li> </ul>   |
| <b>G-Cloud services required</b> | <p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none"> <li>• Lot 2: Cloud software - To continue to provide NGO with a separate instance of case manager to be accessed over the internal and hosted in the cloud under a definition of “Software as a Service”.</li> </ul>  |
| <b>Additional Services</b>       | <p>To provide development works for a training portal via the case manager to be delivered by a third party. An implementation plan is required.</p> <p>The Buyer may need professional services in relation to the software should it need to integrate to other CQC systems in the future</p>   |
| <b>Location</b>                  | <p>The Services will be delivered to the following CQC addresses:</p> <p>Citygate, Gallowgate, Newcastle upon Tyne, NE1 4PA<br/> Seaton House, CityLink, Nottingham, NG2 4LA<br/> 2<sup>nd</sup> Floor, 2 Redman Place, London, E20 1JQ<br/> NICE, Level 1A, City Tower, Piccadilly Plaza, Manchester, M1 4BT<br/> Temple Quaye House, 2 The Square, Bristol BS1 6PN<br/> 15th floor, McLaren Building, 46 Priory Queensway, Dale End, Birmingham, B4 7LR<br/> St Paul’s House, 23 Park Square South, Leeds, LS1 2ND.</p> |
| <b>Quality standards</b>         | <p>The quality standards required for this Call-Off Contract are ISO:27001 and ISO:9001 and CESG and the Supplier will comply with any standards in the Call-Off Contract in particular, clause 14 of Part B (Terms and Conditions and Section 4 (How Services will be delivered) of the Framework Agreement, and with Good Industry Practice.</p>  |

| <p><b>Technical standards:</b></p>     | <p>The Supplier is to comply with all referenced technical standards provided by the Buyer in Schedule 1.</p>   |                |                          |  |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
|--|---|----------------|--------------------------|--|--------------------------|----------|---|---------------------------------------|---------|---|--|---|-------------------------------|---------|----|--|---|------------------------------|---------|----|--|---|-----------------------|---------|--------------|--|
| <p><b>Service level agreement:</b></p> | <p>The service level and availability criteria required for this Call-Off Contract are in the Service Description.</p> <p>Service Levels Support and availability</p> <p>The service includes support to the customer that covers usage of the system and all matters relating to its availability. This support is provided via telephone and email between the hours of 9 am and 5 pm Monday to Friday, excluding English public holidays. Support outside these core hours is available at additional cost. The service is designed to be fast and responsive and has a maximum target response time of 1 second for all page load times. Availability of the service is targeted to exceed 99%.</p> <p>The following service Levels are standard for the provision of Case Manager:</p> <table border="1" data-bbox="531 1153 1361 1641"> <thead> <tr> <th>Severity Level</th> <th>Definition</th> <th>Response Time</th> <th>Resolution Target (SSHs)</th> <th>Examples</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Failure of business critical function</td> <td>30 mins</td> <td>4</td> <td>Main business use interruption (e.g. unable to process cases or to run reports at month end) • Apparent loss of business critical data</td> </tr> <tr> <td>2</td> <td>Defect in high usage function</td> <td>30 mins</td> <td>16</td> <td>Functional error preventing use of screen within a case (e.g. unable to print notes)</td> </tr> <tr> <td>3</td> <td>Defect in low usage function</td> <td>30 mins</td> <td>40</td> <td>Search returning incorrect results • Failure to send reminder emails</td> </tr> <tr> <td>4</td> <td>Non-functional defect</td> <td>30 mins</td> <td>By Agreement</td> <td>Inconsistent sorting • Unintended print outcome<br/>• Typographical or layout error</td> </tr> </tbody> </table> | Severity Level | Definition               | Response Time  | Resolution Target (SSHs) | Examples | 1 | Failure of business critical function | 30 mins | 4 | Main business use interruption (e.g. unable to process cases or to run reports at month end) • Apparent loss of business critical data | 2 | Defect in high usage function | 30 mins | 16 | Functional error preventing use of screen within a case (e.g. unable to print notes) | 3 | Defect in low usage function | 30 mins | 40 | Search returning incorrect results • Failure to send reminder emails | 4 | Non-functional defect | 30 mins | By Agreement | Inconsistent sorting • Unintended print outcome<br>• Typographical or layout error |
| Severity Level                         | Definition  | Response Time  | Resolution Target (SSHs) | Examples   |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
| 1                                      | Failure of business critical function   | 30 mins        | 4                        | Main business use interruption (e.g. unable to process cases or to run reports at month end) • Apparent loss of business critical data |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
| 2                                      | Defect in high usage function   | 30 mins        | 16                       | Functional error preventing use of screen within a case (e.g. unable to print notes)   |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
| 3                                      | Defect in low usage function  | 30 mins        | 40                       | Search returning incorrect results • Failure to send reminder emails   |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
| 4                                      | Non-functional defect   | 30 mins        | By Agreement             | Inconsistent sorting • Unintended print outcome<br>• Typographical or layout error   |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
| <p><b>Onboarding</b></p>               | <p>N/A</p>  |                |                          |  |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |
| <p><b>Offboarding</b></p>              | <p>The offboarding plan for this Call-Off Contract is at the end of the contract, all data will be passed to the client in a secure manner and in structured data files that enable the data to be migrated to other systems. All data held by IIZUKA will then</p>   |                |                          |  |                          |          |   |                                       |         |   |  |   |                               |         |    |  |   |                              |         |    |  |   |                       |         |              |  |

|   |   |
|---|---|
|   | <p>be destroyed in-line with our ISO:27001 data destruction policy.</p> <p>This may include an exit plan of processes or costs (for example) associated with exiting the Call-Off Contract and data standards for migration. Please refer to the offboarding information found in:</p> <ul style="list-style-type: none"> <li>• in the Supplier's Service Definition</li> </ul> <p>Clause 21 (Exit Plan) and 22 (Handover to Replacement Supplier) of the Call-off Terms and Conditions shall apply.</p>  |
| <p><b>Collaboration agreement</b></p>     | <p>N/A</p>  |
| <p><b>Limit on Parties' liability</b></p> | <p>The annual total liability of either Party for all Property Defaults will not exceed £5,000,000.</p> <p>The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>Clause 24.1 in Part B below applies for a more in-depth definition of Buyer Data Defaults, while still maintaining the definitions and meanings of Buyer Data and Default in Schedule 6: Glossary and Interpretations below.</p> <p>The annual total liability for all other Defaults will not exceed the greater of 125% enter percentage of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>No limitation of liability shall apply to gross negligence and wilful misconduct.</p> |

|                                 |   |
|---------------------------------|---|
| <b>Insurance</b>                | <p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</li> <li>● 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)</li> <li>● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law</li> </ul> |
| <b>Force majeure</b>            | <p>A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 10 consecutive days.</p>   |
| <b>Audit</b>                    | <p>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</p> <p>Clauses 7.4 to 7.13 of the Framework Agreement shall apply</p>   |
| <b>Buyer's responsibilities</b> | <p>The Buyer is responsible to appoint a project lead to oversee the work and liaise with / report to supplier contract manager.</p>  |
| <b>Buyer's equipment</b>        | <p>It is anticipated that the Supplier will provide their own Computer equipment in order to conduct the services unless they request otherwise</p>   |

## Supplier's information

|                                   |   |
|-----------------------------------|---|
| <b>Subcontractors or partners</b> | <p>The following is a list of the Supplier's Subcontractors or Partners.</p> <ul style="list-style-type: none"> <li>• AWS</li> <li>• Rock Kitchen Harris</li> </ul> |
|-----------------------------------|---|

## 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.

|  |   |
|--|---|
| <b>Payment method</b>                    | <p>The payment method for this Call-Off Contract is BACS.</p>   |
| <b>Payment profile</b>                   | <p>The payment profile for this Call-Off Contract is annual in arrears for subscription charges and monthly in arrears for all other development services.</p>  |
| <b>Invoice details</b>                   | <p>The Supplier will issue electronic invoices annually (for subscription charges) annually in advance. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.</p>   |
| <b>Who and where to send invoices to</b> | <p>Invoices will be sent to<br/>           Care Quality Commission<br/>           T70 Payables F175<br/>           Phoenix House<br/>           Topcliffe Lane<br/>           Wakefield<br/>           West Yorkshire<br/>           WF3 1WE.<br/>           Or alternatively emailed to <a href="mailto:sbs.apinvoicing@nhs.net">sbs.apinvoicing@nhs.net</a></p> |
| <b>Invoice information required</b>      | <p>All invoices must include Purchase order number</p>  |
| <b>Invoice frequency</b>                 | <p>Invoice will be sent to the Buyer annually</p>   |



|           | Strategy & architecture | Business change | Solution development & implementation | Service management | Procurement & management support | Client interface |
|-----------|-------------------------|-----------------|---------------------------------------|--------------------|----------------------------------|------------------|
| 1. Follow | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |
| ■         | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |
| ■         | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |
| ■         | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |
| ■         | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |
| ■         | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |
| ■         | ■                       | ■               | ■                                     | ■                  | ■                                | ■                |

**Standards for Consultancy Day Rate cards**

**Consultant's Working Day** – 8 hours exclusive of travel and lunch.

**Working Week** – Monday to Friday excluding national holidays

**Office Hours** - 09:00 – 17:00 Monday to Friday

**Travel and Subsistence** – Included in day rate within M25. Payable at department's standard T&S rates outside M25.

**Mileage** – As above

**Professional Indemnity Insurance** – included in day rate.

## Level Definitions

|          | <b>Autonomy</b>  | <b>Influence</b>  | <b>Complexity</b>  | <b>Business Skills</b>   |
|----------|--|---|--|--|
| 1 Follow | Works under close supervision. Uses little discretion. Is expected to seek guidance in expected situations.  | Interacts with immediate colleagues.  | Performs routine activities in a structured environment. Requires assistance in resolving unexpected problems. | Uses basic information systems and technology functions, applications, and processes. Demonstrates an organised approach to work. Learns new skills and applies newly acquired knowledge. Has basic oral and written communication skills.   |
| 2 Assist | Works under routine supervision. Uses minor discretion in resolving problems or enquiries. Works without frequent reference to others.   | Interacts with and may influence immediate colleagues. May have some external contact with customers and suppliers. May have more influence in own domain.  | Performs a range of varied work activities in a variety of structured environments.                            | Understands and uses appropriate methods, tools and applications. Demonstrates a rational and organised approach to work. Is aware of health and safety issues. Identifies and negotiates own development opportunities. Has sufficient communication skills for effective dialogue with colleagues. Is able to work in a team. Is able to plan, schedule and monitor own work within short time horizons. Absorbs   |
| 3 Apply  | Works under general supervision. Uses discretion in identifying and resolving complex problems and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level. | Interacts with and influences department/project team members. May have working level contact with customers and suppliers. In predictable and structured areas may supervise others. Makes decisions which may impact on the work assigned to individuals or | Performs a broad range of work, sometimes complex and non- routine, in a variety of environments.              | Understands and uses appropriate methods, tools and applications. Demonstrates an analytical and systematic approach to problem solving. Takes the initiative in identifying and negotiating appropriate development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation and procedures. Absorbs and applies technical |

|                 |  |   |   |   |
|-----------------|--|---|---|---|
|                 |  |   |   | systems, and how own role relates to other roles and to the business of the employer or client.   |
| 4 Enable        | Works under general direction within a clear framework of accountability. Exercises substantial personal responsibility and autonomy. Plans own work to meet given objectives and processes.   | Influences team and specialist peers internally. Influences customers at account level and suppliers. Has some responsibility for the work of others and for the allocation of resources. Participates in external activities related to own specialism. Makes decisions which influence the success of projects and team objectives. | Performs a broad range of complex technical or professional work activities, in a variety of contexts.  | Selects appropriately from applicable standards, methods, tools and applications. Demonstrates an analytical and systematic approach to problem solving. Communicates fluently orally and in writing, and can convey complex technical information to both technical and non-technical audiences. Facilitates collaboration between stakeholders who share common objectives. Plans, schedules and monitors work to meet time and quality targets and in accordance with relevant legislation and procedures. Rapidly absorbs new technical information and applies it effectively. Has a good appreciation of the wider field of information systems, their use in relevant employment areas and how they relate to the business activities of the employer or client. |
| 5 Ensure/Advise | Works under broad direction. Is fully accountable for own technical work and/or project/ supervisory responsibilities. Receives assignments in the form of objectives. Establishes own milestones and team objectives, and delegates responsibilities. Work is often self-initiated. | Influences organisation, customers, suppliers and peers within industry on the contribution of own specialism. Has significant responsibility for the work of others and for the allocation of resources. Makes decisions which impact the success of assigned projects i.e. results, deadlines and budget. Develops business         | Performs a challenging range and variety of complex or professional work activities. Undertakes work which requires the application of principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/ organisational requirements. | Advises on the available standards, methods, tools and applications relevant to specialism and can make correct choices from alternatives. Analyses, diagnoses, designs, plans, executes and evaluates to time, cost and quality targets. Communicates effectively, formally and informally, with colleagues, subordinates and customers. Demonstrates leadership. Facilitates collaboration between stakeholders who have diverse objectives. Understands the relevance of own area of responsibility/ specialism to the employing organisation. Takes customer requirements   |

|                            |   |  |   |  |
|----------------------------|---|--|---|--|
|                            |   | customers.   |   | initiative to keep skills up to date. Mentors more junior colleagues. Maintains an awareness of developments in the industry. Analyses requirements and advises on scope and options for operational improvement. Demonstrates creativity and <del>innovation in applying solutions for the</del>  |
| 6 Initiate/<br>Influence   | Has defined authority and responsibility for a significant area of work, including technical, aspects. Establishes organisational objectives and delegates responsibilities. Is accountable for actions and decisions taken by self and subordinates. | Influences policy formation on the contribution of own specialism to business significant part of own organisation and influences customers/suppliers and industry at senior management level. decisions which impact the work of employing organisations, achievement of organisational objectives and financial. Develops high-level relationships with customers, suppliers and | Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the formulation wide range of technical and/or management principles.   | Absorbs complex technical information and communicates effectively at all levels to both technical and non-technical audiences. Assesses and evaluates risk. Demonstrates clear leadership and the to influence and persuade. Has a broad understanding of all aspects of IT and deep understanding of own specialism(s). Understands and communicates the role impact of IT in the employing organisation and promotes compliance with relevant legislation. Takes the initiative to keep both own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry. |
| 7 Set Strategy/<br>Inspire | Has authority and responsibility for all aspects of a significant area of work, including policy formation and application. Is fully accountable for actions taken and decisions made,  | Makes decisions critical organisational success. Influences developments within the IT industry at the highest levels. Advances the knowledge and/or exploitation of IT within one or more organisations.  | Leads on the formulation and application of strategy. Applies the highest level of and leadership skills. Has a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment. | Has a full range of strategic management and leadership skills. Understands, explains and presents technical ideas to both technical and non-technical audiences at all levels up to the highest in a persuasive and convincing manner. Has a broad and deep IT coupled with equivalent knowledge of the activities of those businesses and other  |

|  |                               |   |  |   |
|--|-------------------------------|---|--|---|
|  | both by self and subordinates | Develops long-term strategic relationships with customers and industry leaders. |  | organisations that use and exploit IT. Communicates the potential impact of emerging technologies on organisations individuals and analyses the risks of using or not using such technologies. Assesses the impact of legislation, and actively promotes compliance. Takes the initiative to keep both own and subordinates' skills IT in own area(s) of expertise. |
|--|-------------------------------|---|--|---|

## Additional Buyer terms

|  |  |
|--|--|
| <b>Performance of the Service and Deliverables</b>                             | Performance of the Service and Deliverables will be in accordance with Schedule 1 and Part B and C                           |
| <b>Guarantee</b>   | N/A  |
| <b>Warranties, representations</b>   | N/A  |
| <b>Supplemental requirements in addition to the Call-Off terms</b>             | N/A  |
| <b>Alternative clauses</b>   | N/A  |
| <b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b> | N/A  |
| <b>Public Services Network (PSN)</b>   | N/A  |
| <b>Personal Data and Data Subjects</b>   | Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1 applicable. Annex 2 not applicable |

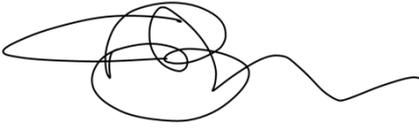
### 1. Formation of contract

- 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.

|                  |   |  |
|------------------|---|--|
| <b>Signed</b>    | Supplier  | Buyer  |
| <b>Name</b>      | ██████████  | ████████████████████   |
| ██████           | ████  | ████████████████████e NHS  |
| <b>Signature</b> |  |  |
| <b>Date</b>      | 8 <sup>th</sup> February 2022   | 16 <sup>th</sup> February 2022   |

## Schedule 1: Services

### Background

This document is a proposal to the Care Quality Commission to extend the usage of the Case Manager system currently used by the Legal Services team to cover the National Guardian's Office. The option under offer is to create a separate instance of Case Manager, hosted under the same agreement and infrastructure for the National Guardian's Office (NGO).

The requirements outlined in this document have been gathered during 2 meetings with key members of staff.

### Staff Members:

J ██████████  
 ██████████  
 ██████████  
 ██████████  
 ██████████  
 ██████████

### Outline of the Requirements

#### Description of usage

Training, managing and dealing with Guardians in all organisations. Responding to enquiries and conducting reviews.

#### In Scope Requirements

- Database of guardians with field reflecting current guardianship status
- Generation of public guardian directory for posting to website
- Responding to enquiries
- Conducting Reviews

- Scheduling and recording training of guardians
- Enquiries can be from public, guardians, workers, other organisations, government e.g. mp
- Association of relevant organisation(s) with enquiries
- Classify people as public, guardians, organisation staff etc.
- Enquiries may be from workers and involve guardians. In this situation the worker is the client.
- Enquiries dealt with through separate case types for complaint, FOI, safeguarding, subject access request, request for training, enrolment as guardian
- Trained people become listed in the directory of guardians if they accept the position
- Recording Qualifying Disclosures as part of associated case/enquiry
- Data portal for quarterly submission of data by guardians

#### **Types of organisations/people dealt with:**

- Workers
- Workers (NHS staff)
- Unions
- Volunteers
- Agency staff
- Students
- Private providers (cqc providers)
- Primary care (GPs etc) (from next April)
- Adult Social Care (date tbc)
- Government
- Trusts
- Regulators
- Arms length bodies
- Professional bodies
  - GMC
  - NMC
  - GDC
  - FODO
  - Pharmacy

#### **Reviews**

- Separate log of reviews
- Workflow for reviews:
  - Preparation
  - Decision
  - Announcement
  - Planning
  - Visits or virtual engagement using teams
  - Drafting
  - Publication
  - Action plan drafting
  - Action plan publication

Case reviews may result in need for communications. Comms team will become involved with the case and collaborate with the organisation(s) involved.

~~Case review is triggered by referral; usually by email or telephone from NHS workers, but can be public.~~

Reviews are triggered by data. It may well be that a document template will be used to assist the decision making process

Correspondence occurs with other agencies to get their input about the review.

Attach documents (surveys, correspondence from the press)

There is a decision regarding of whether to conduct a review.. May require more information.

~~If not going ahead then feedback decision.~~

If it goes ahead then it may be appropriate to formally notify senior leaders at the organisation ~~the CEO of the trust~~ about the review.

Schedule for review may be shared with the organisation(s) involved ~~trust~~ and would ~~is to~~ be manually generated as it needs variable time scales.

Attach evidence to cases.

Drafts of reports.

Templates/forms for decision making.

Links to regular information for case workers from system dashboard.

Templates for email correspondence.

Email import from outlook.

Log costs against cases – amount, type etc. used for travel and accommodation costs. Report to output costs.

## Data portal

Storage and processing of quarterly data returns from guardians

Amend the edit function on an annual basis – when requested by the NGO team (for reconciliation window – turned on for 3-4 week period)

Reports for data portal – making amendments to these if/when changes are made to the portal – *Speaking up data – all details - report*

Development time to amend data portal – including adding new fields e.g.

- New professional groups

- Themes of data

- Organisation level

- Removal of professional levels fields

Development time to amend the reports linked to data portal following changes (2 reports)

## Registration and Training of Guardians

Process needed for registering a new guardian and getting details onto mailing system.

Comms team help with dealing with enquiries.

Trainers provide the training to guardians.

Guardians are nominated locally and register as a new guardian.

Record training events and attendees.

Trainees can be workers other than guardians.

Generate directory from guardian info.

Trainees may choose not to take up the post.

Currently training is induction. Likely to do refresher training soon. Potentially in future offer training as corrective action following complaints.

Exit interview when a guardian leaves. Process needed for exiting guardians.

Every trust has to have at least one guardian. Need to track handover between guardians

Some providers need to have guardians, but not all. Do need guardian if on NHS services contract.

Other external organisations may also have guardians, but don't appear on the public list of guardians. These people can be trained with other guardians.

Weekly clinic where guardians get in contact on a Thursday afternoon. Treat as enquiries with 'clinic' channel. Still subject to the same 20 day target.

## Comms

- Database of guardians with field reflecting current guardianship status
- Generation of public guardian directory for posting to website
- Responding to enquiries
- Conducting Case Reviews

- Scheduling and recording training of guardians
- Enquiries can be from public, guardians, NHS workers at trusts, other organisations, government e.g. mp
- Association of relevant trust(s) with enquiries
- Classify people as public, guardians, trust staff etc.
- Enquiries may be from workers and involve guardians. In this situation the worker is the client.
- Enquiries dealt with through separate case types for complaint, FOI, safeguarding, subject access request, request for training, enrolment as guardian
- Trained people become listed in the directory of guardians if they accept the position
- Recording Qualifying Disclosures as part of associated case/enquiry
- Deal with enquiries from journalists – general comms, plus communications about significant reviews

**Types of organisations/people dealt with: Possible duplication may need to incorporate above**

- Workers (nhs staff)
- Unions
- Private providers (cqc providers)
- Primary care (GPs etc) (from next April)
- Government
- Trusts
- Regulators
- Arms length bodies

## **Training**

Trainers provide the training to guardians.

Guardians are nominated locally and register as a new guardian.

Record training events and attendees.

Trainees can be workers other than guardians.

Generate directory from guardian info.

Trainees may choose not to take up the post.

Currently training is induction. Likely to do refresher training soon. Potentially in future offer training as corrective action following complaints.

Exit interview when a guardian leaves. Process needed for exiting guardians.

Every trust has to have at least one guardian. Need to track handover between guardians

Some providers need to have guardians, but not all. Do need guardian if on NHS services contract.

Other external organisations may also have guardians, but don't appear on the public list of guardians. These people can be trained with other guardians.

Weekly clinic where guardians get in contact on a Thursday afternoon. Treat as enquiries with 'clinic' channel. Still subject to the same 20 day target.

## **Comms**

Weekly bulletin to all guardians – generate mailing list from current guardian records. Used to mail merge in external system that authors and sends messages. Used less often now we have a permanent mailing list but this report is still useful for the guardian support team.

Enquiries can be through social media, face to face at meetings etc. These are to be logged as enquiries and apply the same 20 day target can keep but not often used

Can we also add:

- . a report which can be run detailing any changes to the directory (ie email address, name etc) including new names and stepping down/deletions within a time period.
- This is to update the website and the bulletin audience. And for the purpose of mailing lists
- 

## CRM Requirements

~~These are not case management functions and would normally be done in a CRM system. May be possible to find a way to do in Case Manager, but need further analysis for in/out of scope decision. Assumed to be out of scope for current pricing.~~

~~Regular stake holder meetings:~~

- ~~Engagement meetings~~
- ~~Advisory working group. Quarterly meeting with people to inform policy and procedure~~
- ~~Quarterly board meeting~~
- ~~Pan sector industry group~~

~~Tracking of attendance at meetings and general communications with stakeholders (not enquiry/case review related)~~

~~Notes about providers outside context of individual enquiries/case reviews~~

~~Recording of attendance at and notes from meetings may be possible through extension of events database. Not possible with current Case Manager functionality as events are intended to be case/enquiry related~~

## Security

Implemented as a standalone system from CQC due to potential conflicts of interest.

All users within NGO able to access all cases

## Reporting

- Numbers of enquires and case reviews
- Enquiry and case review resolution times
- Numbers and statuses of guardians
- Compliance with case review schedule

## Integration/External Systems

Online system for Guardians to register and manage contact details. This will duplicate records in Case Manager so may need to integrate/synchronise

- Build in 10 Development days at rate card cost to capture the upcoming changes but also be sufficient flexible for the future.

## Out of Scope Requirements

- Policy and strategy document management
- Authoring and sending of bulk Comms messages
- Annual conference management
- Maintain public web pages

## Part B: Additional Services

Training Portal (Storyboard requirements)



32 Pocklington's Walk  
Leicester  
LE1 6BU  
LE1 6BU

0116 233 7500  
@  
[hello@rkh.co.uk](mailto:hello@rkh.co.uk)  
khk  
[rkh.co.uk](http://rkh.co.uk)

# **lizuka/NGO training portal**

## **Overview**

Based on our existing relationship and past experience of delivering a web interface for your Casemanager API, you talked us through a requirement for the National Guardians Office to allow users to complete and submit their training progress through a portal.

## **Wireframes**

Based on what we discussed, we have produced this very rough, very early set of wireframes to visually illustrate how we see the core of the system working. Please see overleaf.



Email address

Password

[Forgotten password?](#)

Log in

Simple login that authenticates with the lizuka API

Points to contact details/procedure for resetting password, rather than providing a self service system (at least at this stage)

# Welcome back



## Stage 1



## Stage 2



## Stage 3



### Latest updates

11 October 2021  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi

9 June 2021  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor

Simple quarterly updates that could be hardcoded into the system to minimise complexity/avoid content management

Clearly labelled progress, potentially with ability to fetch submitted data for previous stages, but clear signposting to the next available action

# Settings

## Personal details

Full name

Email address

Date of birth

01/09/1970

Basic validation can be provided on fields where it makes sense - e.g. entering an email address twice, ensuring text is text, numbers are numbers, and dates are dates. But validation won't call back to the API to make more sophisticated validation checks.

Save changes

## Another section of details

Field name

Simple self service controls for basic details that a user can change about themselves (but not at organisation level above there are multiple users).



## Update your training record

Field name

Predetermined fields for each training record stage can be presented in addition to file uploads as needed

Field name

Upload document

Single files can be

for  
browsed (or  
dragged and dropped if  
needed) individually -  
multiple file uploads for  
one submission is possi-  
ble if the API allows.

## Costs and time scales

Based on what we know and the assumptions we have made below, we do not expect costs for this project to exceed [REDACTED]

| Role       | Rate       | Days       | Cost       |
|------------|------------|------------|------------|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



32 Pocklington's Walk  
Leicester  
LE1 6BU  
LE1 6BU

0116 233 7500  
@  
[hello@rkh.co.uk](mailto:hello@rkh.co.uk)  
**kh k**  
[rkh.co.uk](http://rkh.co.uk)

## Assumptions

In order to produce this estimate, we have had to make some general assumptions about the project. This list may not be exhaustive but has helped us to estimate project complexity.

- we will be provided with basic brand guidelines from which we can create a clean, simple, mobile-friendly responsive interface
- lizuka will provide all details about individual form elements and their groupings
- our application will not store information it access from the underlying database - we are developing a thin layer that acts as an interface between user and API
- the lizuka API is stable, suitably secure, well documented, and features all the methods we will require to achieve the desired interface and features
- the application will only be presenting single user records based on an authentication process
- there will be some moderate direct client involvement between RKH and NGO as needed
- RKH will invoice lizuka for the works carried out as a subcontractor operating under whatever agreement lizuka and NGO have in place

## Part C: Additional Services

# CR350 NGO Case Manager Maintenance

Approval Dates

|                          |  |
|--------------------------|--|
| <b>Approved</b>          |  |
| <b>Customer Approved</b> |  |
| <b>Customer Accepted</b> |  |

New

## Customer Change Request

|  |  |
|--|--|
| <b>Change Request No.</b>                  | CR350  |
| <b>Change Title</b>                        | NGO Case Manager Maintenance   |
| <b>Information Security Classification</b> | CUSTOMER   |
| <b>Customer Organisation</b>               | National Guardians Office  |
| <b>Customer Contact</b>                    | Jerina Brown, <a href="mailto:Jerina.Brown@nationalguardianoffice.org.uk">Jerina.Brown@nationalguardianoffice.org.uk</a><br>Ellie Staite, <a href="mailto:Ellie.Staite@nationalguardianoffice.org.uk">Ellie.Staite@nationalguardianoffice.org.uk</a> |
| <b>Solution/Product Owner</b>              | <a href="#">Pete Patel</a>   |
| <b>Project/Phase</b>                       | Case Manager   |
| <b>Systems Affected</b>                    | Case Manager   |
| <b>Change Type</b>                         | Configuration / Data   |
| <b>JIRA Issue</b>                          |  <a href="#">CM-4186</a> - CR350 NGO Case Manager Maintenance Identified  |
| <b>CRM ID</b>                              | <a href="#">1164</a>   |

## Reason for Change

NGO have identified a number of required changes/issues with their current Case Manager configuration. See attached [211021 iizuka Issues v1.xlsx](#) & [20211109 NGO-IIZUKA change request doc.docx](#).

## Outcome

The NGO Case Manager system will be updated inline with current requirements.

## Description

The following changes have been identified;

| <b>Definition</b>                      | <b>Notes</b>  | <b>Essential / Desirable</b> | <b>Covered Under Support &amp; Maintenance?</b> |
|--|---|------------------------------|---|
| Clean up of definitions                |   | Essential                    | Yes   |
| Clean up of users on system            | Clean up of users on system/where they sit in the NGO structure on the IIZUKA site. Also user permissions to ensure all users are seeing the workflows that are relevant to them. | Essential                    | Yes   |
| Word changes to drop down lists        |   | Essential                    | Yes   |
| Matching fields with current processes |   | Essential                    | Yes   |
| Add Phone Log themes                   |   | Essential                    | No  |

|   |   |                  |            |
|---|---|------------------|------------|
| <p>Reports - customised reports could be built in-house with training</p> | <p>Further reports and administration training required</p> <ul style="list-style-type: none"> <li>• A report that shows when organisations do not have a Guardian against them</li> <li>• A report that removes organisations if they do not have a Guardian against them</li> <li>• On current reports, telephone numbers do not report with a '0' at the beginning, which makes the report harder to use and time-consuming (currently manually editing the numbers to ensure they appear correctly on our Guardian map).</li> </ul> | <p>Essential</p> | <p>Yes</p> |
| <p>Training - reports and administration training required</p>            | <p>Training tab on external site – development of new workflow internally</p> <ul style="list-style-type: none"> <li>• The inclusion of a 'Training' option once Guardians are registered and logged in to the external site. This would link into an internal workflow on training/competency of Guardians that would be managed by the Guardian Support and Policy team.</li> </ul>   | <p>Essential</p> | <p>No</p>  |
| <p>Outlook interface - With CQC/Little Fish to support changes</p>        | <p>Outlook interface</p> <ul style="list-style-type: none"> <li>• This request is already with CQC/Little Fish to understand how these changes can be implemented. Any update?</li> </ul>   | <p>Desirable</p> | <p>Yes</p> |

|   |   |           |     |
|---|---|-----------|-----|
| Complaints - If the workflow changes will the system be able to cope with the change (to be explored post Enquiries team reviewing complaints process)                      |   | Desirable | No  |
| Registration - Guardian's input their org name leading to mismatching on org name. Organisation name - tool tips needed to ensure 'legal entity' name is used by Guardians. | <p>Guardian registration on external site</p> <ul style="list-style-type: none"> <li>Guidance tips on Guardian registration page needed to ensure Guardians register using their organisation's full legal name, rather than any acronyms or other definitions</li> </ul>   | Essential | Yes |
| Type of organisation - to be reviewed (drop down)   | Review of types of organisations  | Desirable | Yes |
| Advice Clinic to be change to Guardian Support Call   | <p>'advice clinic' to be changed to 'Guardian support call' in all workflows</p> <ul style="list-style-type: none"> <li>These requests involve the editing and clean up of wording, drop downs and pick lists on the NGO's internal case manager workflows, as the offices processes have moved on since the system was created.</li> </ul> | Essential | Yes |

|  |  |                  |            |
|--|--|------------------|------------|
| <p>File notes - Add field - theme of call to support data collection, reporting and evaluation - drop down list (internal)</p>   | <p>Guardian verification process</p> <ul style="list-style-type: none"> <li>• This is currently cumbersome in terms of the time it takes to complete the verification process when Guardians register on the external site. Is this something IIZUKA could help us review to see if the process could be simplified?</li> <li>• Verification of Guardians - currently cumbersome in terms of time it takes. Ask to review with Iizuka and simplify if possible.</li> </ul> | <p>Essential</p> | <p>No</p>  |
| <p>Guardian Report - telephone numbers do not report with a 0 at the beginning making their use difficult and time consuming</p> |  | <p>Essential</p> | <p>Yes</p> |
| <p>Self management - guardian profile (does this work?)</p>  | <p>Guardian profile page on external site</p> <ul style="list-style-type: none"> <li>• Can this become self managing? Could Guardians have the ability to make changes to their email address/phone number?</li> </ul>   |                  | <p>No</p>  |

|  |  |                  |            |
|--|--|------------------|------------|
| <p>Guardian Engagement Workflow - Are the fields used? Review internally and develop this area further</p>   | <p>Guardian engagement workflow addition</p> <ul style="list-style-type: none"> <li>• Addition of a field called ‘theme of call’ that may involve a text box, pick lists and drop down to support data collection, reporting and evaluation.</li> <li>• The entire workflow needs reviewing in order to make sure it is serving the team effectively <b>This may not come under the current contract but is essential work.</b></li> </ul> | <p>Essential</p> | <p>No</p>  |
| <p>Client details page - check that the fields are relevant. Review internally and develop this area further.</p>  | <p>Client details page on internal system</p> <ul style="list-style-type: none"> <li>• Could we check that all fields are still relevant for NGO use and whether this can be reviewed.</li> </ul>  | <p>Desirable</p> | <p>Yes</p> |
| <p>Closed orgs - can we have a marker for when an org has closed? Would help with reporting if we could mark a closed orgs and omit them from reports as required. (linked to reporting question)</p>                                  |  | <p>Essential</p> | <p>Yes</p> |
| <p>Email addresses - If someone leaves an org but used a generic e-mail this is linked to their specific client record. If someone else tries to register/log with the same e-mail address it won't let them. Can this be changed?</p> | <p>Guardian email address issue</p> <ul style="list-style-type: none"> <li>• If someone leaves an organisation but used a group email address (e.g. <a href="mailto:speakup@nhs.net">speakup@nhs.net</a> – this is linked to their specific client record on IIZUKA. If someone else tries to register with the same email address they are not able to. Can this be reviewed at all?</li> </ul>   | <p>Desirable</p> | <p>No</p>  |

|  |   |           |     |
|--|---|-----------|-----|
| <p>Timing out - security issue - has been lengthened to 40mins. Can this be longer?</p>  | <p>Time out of data submission page</p> <ul style="list-style-type: none"> <li>This has been lengthened to 40 minutes but is there any scope to extend this further? Alternatively, more guidance notes needed on Data Submission external page to ensure Guardians are aware of time out.</li> </ul>   | Desirable | Yes |
| <p>Guardians stepping down - Is there a way to flag an org which does not have a guardian? Could then report on this. (links to portal)</p>  | <p>Guardian step-down process via external site to internal site</p> <ul style="list-style-type: none"> <li>Guardians to be able to let the NGO know when they are stepping down – a workflow similar to the NGO Directory and Data Collection where actions can stem from this information. This may not come under the current contract but is essential work.</li> </ul> | Desirable | Yes |
| <p>Could the guardian inform us when stepping down, via a self serve link on iisuka, which will highlight this to us via the enquiries e-mail and trigger the exit process, prior to the guardian stepping down?</p> |   | Essential | Yes |
| <p>Aspects of the E&amp; T guide be included and recorded such as competency level and date of review</p>  |   | Desirable | N/A |
| <p>Removal of option to not be on the public directory and consent to share</p>  | <p>CQC information governance have now given the go ahead.</p>  | Essential | Yes |

|  |  |                  |            |
|--|--|------------------|------------|
| <p>Additional functionality required whereby a Guardian is able to be linked to multiple organisations. Data set to be provided (potential to use CQC provider data which is +4000 records).</p> |  | <p>Essential</p> | <p>Yes</p> |
|--|--|------------------|------------|

## Specification

Give a highly detailed plan of the change to be made covering functional, technical and procedural changes or provide a reference to an external specification document.

## Security

Demonstrate that all reasonably expected security issues resulting from this change have been controlled, or show that none exist.

## Testing

**Test owner:** (replace with the name or role of the person who owns the testing of this change)

## Functional Testing

Describe the plan for functionally testing this change or give reference to an external change plan.

## Security Testing

Describe the testing that will be performed to ensure that all security aspects of the change are verified.

## Impact

Describe the impact of implementing the change on other things such as:

- Procedures and policies
- Employees
- IIZUKA
- Customers
- Systems/assets

- Application downtime

If any *MajorVersion* issues are included in the update being deployed then the deployed is a *Major Update* and must not be attempted without organising a period of outage with the customer or system owner

## Risk Assessment

List risks identified through the risk assessment or by the CAB (if any) and the controls required to treat those risks. Consider whether any of the risks affect the Risk Treatment Plan.

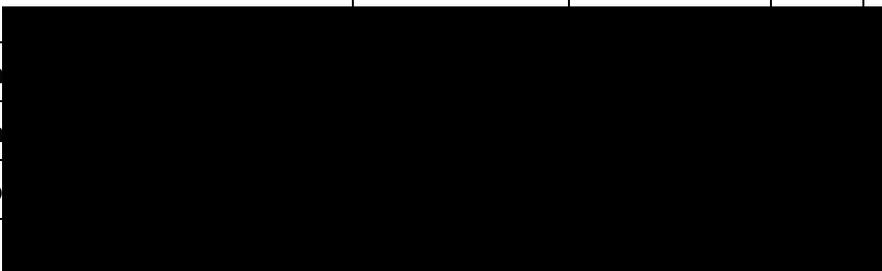
| Confidentiality  |                     | Integrity   |          | Availability  |                     | Quality  |  |
|--|---------------------|---|----------|---|---------------------|--|--|
| Describe the risks of this change related to confidentiality |                     | Describe the risks of this change related integrity |          | Describe the risks of this change related to availability |                     | Describe the risks of this change related to quality |  |
| Uncontrolled   |                     |   |          | Controlled  |                     |  |  |
| Risk   | Impact              | Likelihood  | Controls | Impact  | Likelihood          |  |  |
|  | Low / Medium / High | Low / Medium / High                                 |          | Low / Medium / High                                       | Low / Medium / High |  |  |

## Back Out Procedure

If applicable, define the procedure for backing out the change in the event of failure of acceptance into an operational system.

## Effort & Price

The table below shows the price for this change from any effort involved or line item costs. All prices are in UK Sterling and are exclusive of VAT.

|     |  |  |  |
|-----|--|--|--|
|     |  |  |  |
| Con |  |  |  |
| Con |  |  |  |
| Rep |  |  |  |
|     |  |  |  |

## Acceptance

This change can only be put into service on a live operational environment following completion of all testing documented above and when signed acceptance has been recorded by [Pete Patel](#) on behalf of the customer.

**Guidance changes – for the data portal:**

1. Removal of the professional levels categories
2. Addition of category 'Number of cases related to inappropriate attitudes and behaviours'
3. The category 'Number of cases related to worker safety' to be amended to 'Number of cases related to worker safety and wellbeing'
4. The professional group category to be amended to professional/worker group.  
The options for professional/worker group category to be updated to include the following only:  
Additional Clinical Services  
Additional Professional Scientific and Technical  
Administrative and Clerical  
Allied Health Professionals  
Estates and Ancillary  
Healthcare Scientists  
Medical and Dental  
Nursing and Midwifery Registered  
Students  
Other  
Not known  
These changes are to be made in Q2 2022/23
5. These changes would also need to be reflected in the reports which pull from the portal data 'All Quarterly Data Submission Data' and 'Speaking up Data – All Details' – Report'

**Organisation classification across case Management System**

1. Addition of an organisation category (in addition to the existing organisation type) field in registration, case record and data portal

| Category                   | Type of Organisation/Example |
|----------------------------|------------------------------|
| Commissioning Organisation | Clinical Commissioning Group |
|                            | Commissioning Support Unit   |
| National Body              | Other                        |
|                            | System Regulator             |
|                            | Professional Regulator       |
| Hospital                   | NHS Trust/ Foundation Trust  |
|                            | Independent Hospital         |

|  |                                 |
|--|---------------------------------|
| Integrated care system body              | ICB                             |
|  | ICS                             |
| Primary Care Organisation (Non-provider) | Primary Care Network            |
|  | Local Dental Committee          |
|  | GP Federation                   |
| Primary Care Provider                    | GP Practice                     |
|  | General Dental Practice         |
|  | General Optical Practice        |
|  | General Pharmaceutical Practice |
|  | Private Ambulance               |
|  | Diagnostic and Imaging Service  |
|  | Urgent Care Centre              |
| Care Provider                            | Nursing Home                    |
|  | Care Home                       |
|  | Hospice                         |
| Other                                    | Defence Medical Service         |

These changes would also need to be reflected in the reports which pull from the portal data 'All Quarterly Data Submission Data' and 'Speaking up Data – All Details' – Report'

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

|              |  |                   |                   |
|--------------|--|-------------------|-------------------|
| T            |  |                   |                   |
|              |  |                   |                   |
|              |  |                   |                   |
|              |  |                   |                   |
|              |  |                   |                   |
|              |  |                   |                   |
| <b>Total</b> |  | <b>£60,494.00</b> | <b>£72,592.80</b> |

## Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link;

[G-Cloud 12 Customer Benefits Record](#)

## Part B: Terms and conditions

### 1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

### 2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection)

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

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

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

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

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

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

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

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

### 3. Supply of services

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

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

### 4. Supplier staff

4.1 The Supplier Staff must:

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

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

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

- 4.1.4 respond to any enquiries about the Services as soon as reasonably possible
- 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer
- 4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

## 5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
  - 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
  - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
  - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
  - 5.1.4 have entered into the Call-Off Contract relying on its own due diligence

## 6. Business continuity and disaster recovery

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

- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

## 7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

## 9. Insurance

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

9.2 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: NOT USED



## Schedule 4: NOT USED

1.

Schedule 5: NOT USED

[

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

| Expression                  | Meaning   |
|-----------------------------|---|
| <b>Additional Services</b>  | 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.   |
| <b>Admission Agreement</b>  | The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).   |
| <b>Application</b>          | The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).   |
| <b>Audit</b>                | An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).   |
| <b>Background IPRs</b>      | <p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• created by the Party independently of this Call-Off Contract, or</li> </ul> <p>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.</p> |
| <b>Buyer</b>                | The contracting authority ordering services as set out in the Order Form.   |
| <b>Buyer Data</b>           | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.   |
| <b>Buyer Personal Data</b>  | The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.   |
| <b>Buyer Representative</b> | The representative appointed by the Buyer under this Call-Off Contract.   |

|   |  |
|---|--|
| <b>Buyer Software</b>                     | 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.  |
| <b>Call-Off Contract</b>                  | 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.  |
| <b>Charges</b>                            | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.  |
| <b>Collaboration Agreement</b>            | 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.  |
| <b>Commercially Sensitive Information</b> | 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.   |
| <b>Confidential Information</b>           | Data, Personal Data and any information, which may include (but isn't limited to) any: <ul style="list-style-type: none"> <li>• 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</li> <li>• other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul> |
| <b>Control</b>                            | 'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.   |
| <b>Controller</b>                         | Takes the meaning given in the GDPR.   |
| <b>Crown</b>                              | 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.   |

|   |   |
|---|---|
| <b>Data Loss Event</b>                          | 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.  |
| <b>Data Protection Impact Assessment (DPIA)</b> | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.   |
| <b>Data Protection Legislation (DPL)</b>        | Data Protection Legislation means:<br>(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time<br>(ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy<br>(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  |
| <b>Data Subject</b>                             | Takes the meaning given in the GDPR   |
| <b>Default</b>                                  | Default is any: <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• 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</li> </ul> <p>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.</p> |
| <b>Deliverable(s)</b>                           | The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.  |
| <b>Digital Marketplace</b>                      | The government marketplace where Services are available for Buyers to buy. ( <a href="https://www.digitalmarketplace.service.gov.uk/">https://www.digitalmarketplace.service.gov.uk/</a> )  |
| <b>DPA 2018</b>                                 | Data Protection Act 2018.   |
| <b>Employment Regulations</b>                   | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.   |
| <b>End</b>                                      | Means to terminate; and Ended and Ending are construed accordingly.   |

|  |  |
|--|--|
| <b>Environmental Information Regulations or EIR</b>      | 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.   |
| <b>Equipment</b>   | 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.  |
| <b>ESI Reference Number</b>                              | The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.  |
| <b>Employment Status Indicator test tool or ESI tool</b> | 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:<br><a href="https://www.gov.uk/guidance/check-employment-status-for-tax">https://www.gov.uk/guidance/check-employment-status-for-tax</a>   |
| <b>Expiry Date</b>                                       | The expiry date of this Call-Off Contract in the Order Form.   |
| <b>Force Majeure</b>                                     | <p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• 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</li> <li>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>• 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</li> </ul> |
| <b>Former Supplier</b>                                   | 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).   |
| <b>Framework Agreement</b>                | The clauses of framework agreement RM1557.12 together with the Framework Schedules.   |
| <b>Fraud</b>                              | 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.   |
| <b>Freedom of Information Act or FoIA</b> | 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.   |
| <b>G-Cloud Services</b>                   | 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. |
| <b>GDPR</b>                               | General Data Protection Regulation (Regulation (EU) 2016/679)   |
| <b>Good Industry Practice</b>             | 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.               |
| <b>Government Procurement Card</b>        | The government's preferred method of purchasing and payment for low value goods or services.  |
| <b>Guarantee</b>                          | The guarantee described in Schedule 5.  |
| <b>Guidance</b>                           | 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.  |

|   |   |
|---|---|
| <b>Implementation Plan</b>                    | 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.   |
| <b>Indicative test</b>                        | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.  |
| <b>Information</b>                            | Has the meaning given under section 84 of the Freedom of Information Act 2000.  |
| <b>Information security management system</b> | The information security management system and process developed by the Supplier in accordance with clause 16.1.  |
| <b>Inside IR35</b>                            | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.   |
| <b>Insolvency event</b>                       | Can be: <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> </ul>  |
| <b>Intellectual Property Rights or IPR</b>    | Intellectual Property Rights are: <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> <li>• all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul> |
| <b>Intermediary</b>                           | For the purposes of the IR35 rules an intermediary can be: <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>  |

|                           |  |
|---------------------------|--|
| <b>IPR claim</b>          | As set out in clause 11.5.   |
| <b>IR35</b>               | 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.  |
| <b>IR35 assessment</b>    | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.   |
| <b>Know-How</b>           | 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.  |
| <b>Law</b>                | 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. |
| <b>LED</b>                | Law Enforcement Directive (EU) 2016/680.   |
| <b>Loss</b>               | 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 ' <b>Losses</b> ' will be interpreted accordingly.  |
| <b>Lot</b>                | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.   |
| <b>Malicious Software</b> | 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.                                   |
| <b>Management Charge</b>  | 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.  |

|                                 |  |
|---------------------------------|--|
| <b>Management Information</b>   | The management information specified in Framework Agreement section 6 (What you report to CCS).  |
| <b>Material Breach</b>          | 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. |
| <b>Ministry of Justice Code</b> | 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.                              |
| <b>New Fair Deal</b>            | 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.                |
| <b>Order</b>                    | An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.  |
| <b>Order Form</b>               | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.   |
| <b>Ordered G-Cloud Services</b> | G-Cloud Services which are the subject of an order by the Buyer.   |
| <b>Outside IR35</b>             | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.                                  |
| <b>Party</b>                    | The Buyer or the Supplier and 'Parties' will be interpreted accordingly.   |
| <b>Personal Data</b>            | Takes the meaning given in the GDPR.   |
| <b>Personal Data Breach</b>     | Takes the meaning given in the GDPR.   |
| <b>Processing</b>               | Takes the meaning given in the GDPR.   |
| <b>Processor</b>                | Takes the meaning given in the GDPR.   |

|                                       |  |
|---------------------------------------|--|
| <b>Prohibited act</b>                 | <p>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:</p> <ul style="list-style-type: none"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul> |
| <b>Project Specific IPRs</b>          | <p>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.</p>   |
| <b>Property</b>                       | <p>Assets and property including technical infrastructure, IPRs and equipment.</p>   |
| <b>Protective Measures</b>            | <p>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.</p>  |
| <b>PSN or Public Services Network</b> | <p>The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.</p>   |
| <b>Regulatory body or bodies</b>      | <p>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.</p>  |
| <b>Relevant person</b>                | <p>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.</p>  |
| <b>Relevant Transfer</b>              | <p>A transfer of employment to which the employment regulations applies.</p>   |

|                                 |   |
|---------------------------------|---|
| <b>Replacement Services</b>     | 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.   |
| <b>Replacement supplier</b>     | 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).  |
| <b>Security management plan</b> | The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.   |
| <b>Services</b>                 | The services ordered by the Buyer as set out in the Order Form.   |
| <b>Service data</b>             | Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.  |
| <b>Service definition(s)</b>    | 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.   |
| <b>Service description</b>      | The description of the Supplier service offering as published on the Digital Marketplace.   |
| <b>Service Personal Data</b>    | 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.  |
| <b>Spend controls</b>           | The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a> |
| <b>Start date</b>               | The Start date of this Call-Off Contract as set out in the Order Form.  |
| <b>Subcontract</b>              | 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.   |

|                                |  |
|--------------------------------|--|
| <b>Subcontractor</b>           | 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. |
| <b>Subprocessor</b>            | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.   |
| <b>Supplier</b>                | The person, firm or company identified in the Order Form.  |
| <b>Supplier Representative</b> | The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.   |
| <b>Supplier staff</b>          | 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.                        |
| <b>Supplier terms</b>          | 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.  |
| <b>Term</b>                    | The term of this Call-Off Contract as set out in the Order Form.   |
| <b>Variation</b>               | This has the meaning given to it in clause 32 (Variation process).   |
| <b>Working Days</b>            | Any day other than a Saturday, Sunday or public holiday in England and Wales.  |
| <b>Year</b>                    | 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: Nimali de Silva, Care Quality Commission, 2 Redman Place, 2<sup>nd</sup> Floor, London E20 1JQ
- 1.2 The contact details of the Supplier's Data Protection Officer is: Mike Atkin Ilzuka Software Technologies, 2 Church Court, Cox Street, Birmingham, B31RD
- 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 | <p><b>The Buyer is Controller and the Supplier is Processor</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>● National Guardian Office Case Management System</li> </ul> |
| Duration of the Processing                                | 1 <sup>st</sup> December 2021 to 30 <sup>th</sup> November 2023 and any extensions   |
| Nature and purposes of the Processing                     | <p>All documentation relating to correspondence and case reviews will be stored in the system. Case data includes full case history including personal details, notes, correspondence, case actions, images.</p> <p>This information will be obtained as it currently is from external individuals seeking advice and</p>  |

|  |   |
|--|---|
|  | <p>support, as well as any legal matters and challenges that are brought to NGO's attention by external parties. The National Guardian's Office case management system is only accessible to National Guardian Office staff. There will be no transfer of information out of the system, except where required to respond to legal cases.</p>   |
| Type of Personal Data  | <p>Individuals' contact details ie telephone numbers and email addresses:</p> <p>Data that will be collected will include the following information:</p> <p>Protected Disclosures Act 2014</p> <p>Qualifying disclosures</p> <p>Legal issues</p> <p>Health/Patient history</p> <p>Speaking up Concerns</p> <p>Training enquiries</p>  |
| Categories of Data Subject   | <p>NGO staff</p> <p>Health and Care Provider staff</p> <p>Freedom to Speak up Guardians,</p> <p>Individuals contacting the NGO</p> <p>Employees of CQC only.</p>  |
| 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 | <p>The information stored on the server and cloud based system will adhere to the KIM retention and disposal schedule as there will be a functionality within the LCMS that has a date and time calculator of how long the information has been retained for so that when the time comes, the information can be disposed of.</p> <p>The retention schedule for all NGO information is held by the KIM teams. The information stored and the duration will be reflected on the asset register, which is held by KIM colleagues.</p> <p>During the last month of the contract NGO will work with iizuka Software Technologies to implement the off boarding and exit strategy to extract the data ready to import into an alternative system. All data will be destroyed within a maximum of 30 days at contract end</p> |

## Annex 2: Joint Controller Agreement

### 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.