Order Form

CALL-OFF REFERENCE:	**CCSH23A01**
THE BUYER:	National Crime Agency (NCA)
BUYER ADDRESS	PO Box 8000, London SE11 5EN
THE SUPPLIER:	Working on Wellbeing Ltd
SUPPLIER ADDRESS:	20 Grosvenor Place London SW1 7HN
REGISTRATION NUMBER:	08544676
DUNS NUMBER:	
SID4GOV ID:	

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 13 December 2023
It's issued under the Framework Contract with the reference number RM6182 Provision of Occupational Health and Employee Assistance Programmes.

CALL-OFF LOT(S):
Lot 1 Fully Managed

CALL-OFF INCORPORATED TERMS
The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

2. The following Schedules in equal order of precedence:

   - Joint Schedules for RM6182
     - Joint Schedule 1 (Definitions)
     - Joint Schedule 2 (Variation Form)
     - Joint Schedule 3 (Insurance Requirements)

- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 8 (Guarantee)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)
- Joint Schedule 12 (Supply Chain Visibility)

- Call-Off Schedules for RM6182
  - Call-Off Schedule 1 (Transparency Reports)
  - Call-Off Schedule 2 (Staff Transfer)
  - Call-Off Schedule 3 (Continuous Improvement)
  - Call-Off Schedule 5 (Pricing Details)
  - Call-Off Schedule 7 (Key Supplier Staff)
  - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - Call-Off Schedule 9 (Security)
  - Call-Off Schedule 10 (Exit Management)
  - Call-Off Schedule 13 (Implementation Plan and Testing)
  - Call-Off Schedule 14 (Service Levels)
  - Call-Off Schedule 15 (Call-Off Contract Management)
  - Call-Off Schedule 16 (Benchmarking)
  - Call-Off Schedule 18 (Background Checks)
  - Call-Off Schedule 20 (Call-Off Specification)

3. CCS Core Terms (version 3.0.10)
4. Joint Schedule 5 (Corporate Social Responsibility)
5. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

1. Official Secrets Act 1911 to 1989, S182 of the Finance Act 1989

1.1 The Supplier shall comply with, and shall ensure that Supplier Staff comply with:

1.1.1 the provisions of the Official Secrets Acts 1911 to 1989; and

1.1.2 the provisions of Section 182 of the Finance Act 1989.

1.2 In the event that the Supplier or the Supplier Staff fail to comply with this clause, the Buyer reserves the right to take any or all of the following actions:

1.2.1 terminate the Contract by giving notice in writing to the Supplier;

1.2.2 to initiate criminal proceedings.

2. Supplier Staff

2.1 The Supplier, and any subcontractors, must have policies and processes in place covering pre and post-employment checks for all staff including compliance with Employment Legislation relating to identity checks and establishing 'right to work' in the UK.

2.2 At the Buyer's written request, the Supplier shall provide a list of the names and addresses of all persons who may be employed on the Contract specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Buyer may reasonably request.

2.3 The Supplier shall comply with the Buyers Staff Vetting Procedures as detailed in the specification in respect of all persons employed or engaged in the provision of the Services.

2.4 The Buyer may, by written notice to the Supplier, refuse to admit onto, or withdraw permission to remain on any of the Buyer's premises:

2.4.1 any member of Supplier Staff; or

2.4.2 any person employed or engaged by any member of the Supplier Staff, whose admission or continued presence would, in the reasonable opinion of the Buyer, be undesirable.

2.5 The Buyer shall not be required to disclose its reasons for considering an individual unsuitable. Any such unsuitability is not an indication that the individual is unsuitable to work on other contracts for the Supplier.

2.6 The decision of the Buyer as to the suitability of any person employed upon this service shall be final and conclusive.

3. Publicity and Branding

3.1 The Supplier shall not (and shall procure that no Subcontractor shall) make any advertisement, public statement or press announcement in relation to this Contract or the provision of the Goods or Services without the Buyer's prior written consent.

3.2 The Supplier shall not use any of the Buyer's Intellectual Property Rights, including (but not limited to) the Buyer's names, branding, domain names, logos or trade marks on any of its products or services or in any promotional, marketing or similar material or advertising without the Buyer's prior written consent.

3.3 The Supplier hereby agrees and acknowledges that the unauthorised use of the Buyer's names, branding, domain names, logos and/or trademarks may breach Crown copyright and that legal action may be taken against it in the event of any unauthorised use of such material. This applies to all Buyer-owned brands including (but not limited to) the Buyer's corporate identity, Child Exploitation and Online Protection (CEOP) command brands and/or campaign brands. All requests for external use of a NCA brand must be

approved in writing by the Buyer branding team and the Supplier shall in each case seek to obtain such approval in advance by submitting an approval request to Redacted under FOIA section 40, Personal Information.

3.4 Nothing in this Contract constitutes an endorsement by the Buyer of the Supplier's goods or services, and the Supplier shall not conduct itself in a way that implies any endorsement or authorisation by the Buyer.

4. Freedom of Information

4.1 For the purpose of the FOIA, the Buyer is not a 'public authority'(as listed in Schedule 1 of the Act), and is not under any duty to disclose information. The Buyer is also not listed as a ‘Scottish Public Authority’ in the Freedom of Information (Scotland) Act 2002. In addition any information from, or relating to the Buyer has an absolute exemption from disclosure by other public authorities by virtue of Section 23 of the Act (as amended by the Crime and Courts Act 2013). Any request for information must be referred to the Buyer’s FOI single point of contact, by email to PICUEnquiries@nca.gov.uk or by telephoning 0870 268 8677.

4.2 Additionally, the Buyer will not provide a public authority with any Information in respect of a Request for Information they receive. However, Information received from, (either directly or indirectly), or “relating to” the Buyer that is already held by the public authorities or their subcontractors, has additional protection from release to the public by virtue of section 23 of the FOIA. The Buyer’s Information may also be covered by the FOIA Section 24 exemption, this is applicable to Information the non-disclosure of which is necessary to safeguard national security.

4.3 It is important that the Supplier understands the different legislation covering the Buyer under Section 23 of the FOIA, so as not to inadvertently breach the FOIA.

4.4 The Supplier shall acknowledge the Buyer’s position in respect of the FOIA and agree to assist and co-operate in order to enable the Buyer to best protect its Information. The Supplier shall also ensure that any sub-contract the Supplier enters into also contains a condition in similar terms.

4.5 Failure to comply with this policy may result in an unauthorised disclosure of the Buyer’s information and a potential breach of the Official Secrets Act.

4.6 The provisions of this Clause shall survive termination or expiry of the Contract.

5. Security Measures

5.1 The Supplier shall not, either before or after the completion or termination of this Contract, disclose any information relating to any aspect of the Contract without written Buyer consent.

5.2 The Supplier must provide an Exit Plan within the first 3 months of the contract term which should include how they will manage Buyer assets.

5.3 Without prejudice to the provisions of Clause 5.1, the Supplier shall, both before and after the completion or termination of this Contract, take all reasonable steps to ensure:

5.3.1 that if the Buyer gives notice in writing to the Supplier at any time requiring the delivery to the Buyer of any document, model or item, that document, model or item (including all copies of or extracts therefrom) shall forthwith be delivered to the Buyer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

5.3.2 the Supplier must immediately return to the Buyer all applicable assets, e.g. Buyer access passes, Information and Communication Technologies (ICT) equipment, materials, work or records held, including any back up media unless destruction is agreed in accordance with IA security requirements.

5.4 The decision of the Buyer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of this Clause shall be final and conclusive. Any such decision of the Buyer shall be exercised reasonably and be proportionate to the event. If any dispute arises as to the operation of this clause then the decision will be subject to the disputes resolution process.

5.5 If and when directed by the Buyer, the Supplier shall secure that any person employed by it who is specified by the Buyer, shall be required to sign a statement of understanding of the Official Secrets Act, 1910 to 1989.

5.6 If at any time either before or after the expiry or termination of this Contract it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Buyer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

5.7 The Supplier shall place every person employed by it, other than a Subcontractor, who in its opinion has or will have such knowledge of any Confidential Information as to appreciate its significance, under a duty to the Supplier to observe the same obligations in relation to that information as are imposed on the Supplier, and shall, if directed by the Buyer, place every person who is specified, under the like duty in relation to any such information and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Clause 5.6 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Buyer with all necessary particulars.

5.8 The Supplier shall include in any Sub-Contract provisions in such terms as the Buyer may consider appropriate for placing the Subcontractor under obligations in relation to security corresponding to those placed on the Supplier by

this Clause, but with such variations (if any) as the Buyer may consider necessary. Further the Supplier shall:

5.8.1 give such notices, directions, requirements and decisions to its Subcontractor(s) as may be necessary to bring the provisions relating to security which are included in Sub-Contracts under this Clause 5.7 into operation in such cases and to such extent as the Buyer may direct;

5.8.2 if it becomes aware of any breach by the Subcontractor of the obligations of security included in their Sub-Contracts in pursuance of this Clause, notify such breach forthwith to the Buyer; and

5.8.3 if required by the Buyer, exercise its power to terminate the Sub-Contract under the provision in that Sub-Contract which corresponds to clause 5.11.

5.9 The Supplier shall give the Buyer such information and particulars as the Buyer may from time to time require for the purposes of satisfying the Buyer that the obligations imposed by or under the foregoing provisions of this Clause have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Buyer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Contract or in which there is or will be any item to be supplied under this Contract, and also to inspect any document or item in any such premises or which is being made or used for the purposes of this Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

5.10 Nothing in this Clause shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

5.11 The Buyer may, by notice in writing, terminate this Contract forthwith if the Buyer shall consider that any of the following events has occurred:

5.11.1 that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Clause; or

5.11.2 that the Supplier has committed a breach of any obligations in relation to security imposed upon it by any other contract with the Buyer; or

5.11.3 that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in Clause 5.11.1, Confidential information has been or is likely to be acquired by a person who, in the opinion of the Buyer, ought not to have such information.

5.12 A decision of the Buyer to terminate this Contract in accordance with the provisions of Clause 5.11 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any way to the event or considerations upon which the Buyer's decision is based. Any such

decision of the Buyer on this shall be exercised reasonably and be proportionate to the event. If any dispute arises as to the operation of this clause then the decision will be subject to the dispute resolution process.

5.13 The Supplier may within five (5) Working Days of the termination of this Contract in accordance with the provisions of Clause 5.11, give the Buyer notice in writing requesting the Buyer to state whether the event upon which the Buyer's decision to terminate was based is an event mentioned in Clauses 5.11.1, 5.11.2 or 5.11.3 and to give particulars of that event; and the Buyer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

5.14 The termination of this Contract pursuant to Clause 5.11 shall be without prejudice to any rights of either party which shall have accrued before the date of such termination.

6. Security Requirements and Information Security

6.1 The Supplier, and any sub-contractor must meet all the Buyer's relevant security policies as notified by the Buyer, from time-to-time.

6.2 All staff employed on the Contract, including the Supplier Staff and Subcontractor's staff, must hold the appropriate level of security clearance, as stated by the Buyer (including those set out or referenced in Call-Off Schedule 18 (Background Checks)):

6.2.1 all employees on the Contract must have, as a minimum, BPSS checks without exception,

6.2.2 and basic Disclosure and Barring Service (DBS) checks may also be required for certain roles,

6.2.3 and National Security Vetting (NSV) clearance either at CTC, SC or DV level may be required for certain roles,

6.2.4 and, where applicable, NCA NSV Enhanced Checks and to maintain that clearance throughout the term of the Contract.

6.3 The Supplier and its sub-contractors must comply with all the requirements of ongoing personnel security (aftercare) and exit procedures.

6.4 The Supplier must comply with His Majesty's Government Security Policy Framework and the Government's Security Classification and any amendments or revised editions to this document which may be issued from time-to-time.

6.5 The Supplier shall bring to the attention of the Buyer any business development outside of the Buyer's areas of responsibility which is likely to give rise to a security risk.

6.6 The Supplier shall have in place appropriate security systems and policies at all sites within its organisation, and at any relevant Subcontractor(s), in relation to the handling and storage of any Buyer related documentation and/or assets in accordance with His Majesty's Security Policy.

6.7 The Supplier shall ensure that all HMG Classified information, and specifically personal data, is processed, stored, archived, purged, erased and/or destroyed in accordance with HMG Security Policy. This must align with the National Cyber Security Centre (NCSC) and Centre for the Protection of National Infrastructure (CPNI) guidance and Security Policy Framework (SPF).

6.8 The Supplier shall ensure, and provide written evidence, that an Information Security Policy is in place. The policy shall also cover Confidential Information and Government Data risk. The policy must be communicated to any individuals with access to systems where any Confidential Information and/or Buyer Data are processed.

6.9 The Supplier shall ensure that all access to, and use of, any Government Data or Confidential Information involving Buyer business (including, but not limited to, Personal Data, financial records such as invoices and any other data, as well as the tracking of the assets) shall be controlled and that only authorised personnel shall have access. Robust controls and capabilities for access, auditing and monitoring shall be in place to ensure:

6.9.1 the prevention of attempts to gain access, and

6.9.2 identification of actual unauthorised access.

6.10 The Supplier shall allocate responsibilities for Information Security wherever Buyer business or information or assets are involved and the Supplier shall take all reasonable steps necessary to protect Information Security.

6.11 The Supplier will provide evidence of their Incident Management Plan and, where applicable, review, audit and update their plan in accordance with the Buyer's instructions.

6.12 The Supplier shall report the actions it has taken in respect of a Security Incident, including, but not limited to: investigation, containment and eradication of the cause of the Information Security Incident, to the Buyer and its Security Incident Management Team.

6.13 Where the Supplier uses computer systems to process any Buyer Data (including financial records such as invoices and any other data as well as the tracking of the assets), the Supplier must ensure the confidentiality, integrity and availability of any of Buyer Data that is gathered, processed an stored:

6.13.1 these measures must be in accordance with the 'need to know' and 'need to share' security principles concerning Authority information and data,

6.13.2 including Personal Sensitive information and details relating to Authority procedures and discreet and/or operational procedures.

6.14 Where the Supplier is involved with the transferring of any Buyer related data, such transfer must be controlled, and conform with protection measures appropriate to the impact level and or risk assessment.

6.15 The Supplier must implement and maintain a programme of exercising and testing to validate effectiveness of its business continuity strategies and solutions in line with ISO 22301 BCM (Operations and Planning) including that:

6.15.1 the Supplier must provide a BCDR Plan Review Report at the Year 1 anniversary of the Contract and annually thereafter,

6.15.2 the BCDR Plan Review Report must include decisions to continual improvement opportunities and any need for changes must include details of effectiveness and efficiency measures.

6.16 The Supplier shall consider the physical security requirements of the Buyer at the onset as part of the implementation of the contract in line with the Buyer's guidance and/or recommendations. The Supplier must ensure careful consideration to physical security measures required at Buyer premises and the Supplier's premises to protect Buyer assets, HMG information and data, Crown copyright material, commercial material and operational sensitivity

6.17 The Supplier shall ensure that Buyer Data is held within the United Kingdom and is not capable of being accessed from outside of the United Kingdom.

6.18 The Supplier must not to take NCA data outside of the UK mainland boundary without prior authorisation from the NCA Integrated Protective Security Team. Requests to take NCA data outside of the UK mainland boundary must be made via the NCA Information Assurance and Accreditation team. Approval must be confirmed in writing for each separate occasion. This includes movement of IT devices or removable storage devices.

6.19 The Supplier will not to join online forums or meetings where NCA business is to be discussed from outside of the UK mainland regardless of whether the device being used is owned by the NCA, the supplier or the individual.

7. Environmental Sustainability

7.1 The Supplier shall contribute towards the public sector's goal of improving the sustainability of ICT purchases and their operation via the Goods and/or Services supplied to the Buyer.

7.2 The Supplier shall where required, support the Buyer in developing its environmental policies, by providing advice on the best use of Goods and/or Services supplied and where appropriate by proposing innovative Goods and/or Services.

7.3 The Supplier is required to consider the impacts of their business processes on the environment and take measures to reduce such impact including by supporting where possible the Government's Environmental Policy and Sustainable Development Plan: https://www.gov.uk/government/sustainable-development

8. Energy Efficiency

8.1 The Supplier must consider the energy efficiency of all Goods and/or Services offered to the Buyer and provide appropriate solutions and advice: (a) DEFRA: Sustainability in information and communication technology (ICT): a Defra guide

8.2 Certification of Energy Efficiency for Data Centers: https://www.ceedacert.com/

9. Carbon Footprint Measurement

9.1 The Supplier must provide information on all relevant Goods and Services to assist the Buyer in the task of calculating its total carbon footprint.

9.2 The Supplier must offer itemised carbon footprint figures for all Goods and/or Services.

9.3 External links for guidance: (a) DEFRA: https://uk-air.defra.gov.uk/ (b) PAS2050: http://shop.bsigroup.com/en/forms/PASs/PAS-2050 (c) iSERVcmb: www.iSERVcmb.info

10. Waste Management

10.1 The Supplier shall ensure that they have adequate waste management solutions for the Goods and/or Services.

10.2 The Supplier shall where requested provide the Buyer with a waste management strategy for the Goods and/or Services including refresh, refurbishment or reuse of equipment and environmental recovery, recycling or disposal options.

10.3 External links for guidance: (a) WEEE Directive: http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0096:EN:NOT (b) RoHS Regulations: http://www.rohs.gov.uk/

11. Supplier Accessibility Responsibilities

11.1 Where required by the Buyer, the Supplier shall provide suitable hardware and software to meet the diverse user needs. This may include individuals with a visual, auditory, physical, speech, cognitive, language, learning, behavioral or neurological impairment, as well as the needs of users for whom English is not their first language.

11.2 The Supplier shall assist the Buyer in fulfilling its legal obligations with regards to accessibility, by offering help and guidance on how the Services can either support or be tailored to the Buyer's needs.

11.3 Where required by the Buyer, the Supplier shall provide an accessibility statement for Services provided under a Call Off Contract.

11.4 The Supplier shall where relevant maintain an accessibility policy, and identify (and where requested provide the details to the Buyer) a role or department within their organisations with responsibility for the policy.

12. Modern Slavery

12.1 The Supplier shall at all times be compliant with the provisions of the Modern Slavery Act 2015 External link: http://www.legislation.gov.uk/ukpga/2015/30/contents/enacted

12.2 The Supplier shall annually complete the modern slavery assessment tool as directed by CCS. External link: https://supplierregistration.cabinetoffice.gov.uk/msat

12.3 The Supplier shall make the outcomes of its modern slavery assessment to the Buyer when requested.

12.4 The Supplier shall use the outputs of the modern slavery assessment within their Continuous Improvement Plan.

Clause 10.1.2 of the Core Terms shall be deleted are replaced with the following:

10.1.2 The Relevant Authority can extend the Contract for up to two (2) Extension Periods (as set out in the Order Form) by giving the Supplier no less than three (3) Months' written notice before the Contract or the relevant Extension Period expires.

CALL-OFF START DATE:	No later than 27 November 2024
CALL-OFF EXPIRY DATE:	No later than 26 November 2027
CALL-OFF INITIAL PERIOD:	3 years
CALL-OFF OPTIONAL EXTENSION PERIOD:	2 Years (12 months at a time)

CALL-OFF DELIVERABLES
See details in Call-Off Schedule 20 (Call-Off Specification)

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year are: six hundred thousand pounds (£600,000).

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES

N/A

PAYMENT METHOD

Payment shall be made in accordance with clause 4 of the Core Terms.

BUYER'S INVOICE ADDRESS:

Accounts Payable
Redacted under FOIA section 40, Personal Information

BUYER'S AUTHORISED REPRESENTATIVE
Redacted under FOIA section 40, Personal Information
T: **Redacted under FOIA section 40, Personal Information**
F: **Redacted under FOIA section 40, Personal Information**
M: **Redacted under FOIA section 40, Personal Information**
E: **Redacted under FOIA section 40, Personal Information**

BUYER'S ENVIRONMENTAL POLICY

Not used

BUYER'S SECURITY POLICY

- The Supplier shall comply the NCA Supply Chain and Security Requirements, available on request to the Buyer.
- The Supplier shall comply with the Cyber Essentials Plus (CE+) and Cyber Essentials Requirements for IT infrastructure 2020. [Note to Bidders: If you do not hold Cyber Essentials Plus but hold certification for ISO 27001, the scope must include the controls listed within Cyber Essentials Plus.]
- The Supplier shall comply with the HMG Baseline Personnel Security Standard (BPSS) 2018.
- The Supplier shall comply with the Off-Shoring – Cabinet Office Guidance 2020.

SUPPLIER'S AUTHORISED REPRESENTATIVE
Redacted under FOIA section 40, Personal Information
Redacted under FOIA section 40, Personal Information

SUPPLIER'S CONTRACT MANAGER
Redacted under FOIA section 40, Personal Information

PROGRESS REPORT FREQUENCY
Monthly performance reports are to be provided to the Buyer by the Supplier by the tenth (10^{th}) Working Day in the Month following the Month to which the report relates.

PROGRESS MEETING FREQUENCY
The Supplier is required to attend regular contract review meetings with the Buyer at an agreed location and time.

KEY STAFF
Redacted under FOIA section 40, Personal Information

KEY SUBCONTRACTOR(S)
Redacted under FOIA section 43, Commercial Interests

COMMERCIALLY SENSITIVE INFORMATION
Supplier Tender
Supplier pricing

SERVICE CREDITS
Service Credits will accrue in accordance with Call-Off Schedule 14 (Service Levels). The Service Credit Cap is: 10% of the total monthly invoice value shall be payable in any one month.

The Service Period is: One Month

A Critical Service Level is: a Service Level designated as a Critical Service Level in Annex A to Part A of Call-Off Schedule 14 (Service Levels).

ADDITIONAL INSURANCES
Not applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender).

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	**Redacted under FOIA section 40, Personal Information**	Signature:	**Redacted under FOIA section 40, Personal Information**
Name:	**Redacted under FOIA section 40, Personal Information**	Name:	**Redacted under FOIA section 40, Personal Information**
Role:	**Redacted under FOIA section 40, Personal Information**	Role:	**Redacted under FOIA section 40, Personal Information**

Date:	**Redacted under FOIA section 40, Personal Information**	Date:	**Redacted under FOIA section 40, Personal Information**