G-Cloud 12 Call-Off Contract

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

Part A: Order Form

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

Digital Marketplace service ID number	453785448844410
Call-Off Contract reference	To be confirmed
Call-Off Contract title	Credit Reference Agency Services
Call-Off Contract description	Secure web-based online portal or integrated API service, providing access to a range of information and reporting based on multiple sources of data, including Credit Reference Agency (CRA) Data.
Start date	21st September 2022
Expiry date	20th September 2023
Call-Off Contract value	£1,257,122.86 + VAT
Charging method	Monthly Invoice
Purchase order number	To be confirmed

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

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

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

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

From the Buyer	Secretary of State for Work and Pensions Peel Park Control Centre Brunel Way Blackpool Lancashire FY4 5SE
To the Supplier	Equifax Ltd 1 Angel Court London EC2R 7HJ Company number: 02425920
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Debt Services and Banking Commercial Lead

Name: Sasha Paylor

Email: Sasha.Paylor@dwp.gov.uk

Phone: 0792 020 4628

For the Supplier:

Title: Head of Public Sector Growth

Name: Oliver Abbott

Email: Oliver.Abbott@equifax.com

Phone: 0782 531 3714

Call-Off Contract term

Start date	This Call-Off Contract Starts on **21st September 2022** and is valid for **12 months**
Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for either Party is a maximum of 14 days from the date of written notice for Ending without cause (as per clause 18.1), subject to the following: • the Supplier must provide written notice on or before 19 October 2022 if it wishes to exercise this right, unless agreed otherwise by the Parties; • the notice period will increase to 30 days, from 20 October 2022 for the Buyer; • should the Buyer terminate the Call-Off Contract pursuant to clause 18.1 by providing written notice after 19 October 2022, notwithstanding clause 18.2.2, the Buyer will pay the Supplier the remainder of any fixed Call-Off Contract Charges outlined at Schedule 2.
Extension period	This Call-off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 4 weeks written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.

Buyer contractual details

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

G-Cloud lot	This Call-Off Contract is for the provision of Services under: • Lot 2: Cloud Software
G-Cloud services required	The Equifax Public Sector Gateway The above G-Cloud Services to be provided by the Supplier under the above Lot are further detailed in Schedule 1 (The Services) of this Call-off agreement.
Additional Services	Not Used
Location	The Services will be delivered nationally throughout the UK.
Quality standards:	The quality standards the Supplier is required to satisfy under this Call-Off Contract are those detailed in Schedule 1.
Technical standards:	The technical standards the Supplier is required to satisfy under this Call Off Contract are those specified in Schedule 1.
Service level agreement:	The service level and availability requirements the Supplier is required to satisfy for this Call-Off Contract are those specified at clauses 5 and 11 (Service Levels and Performance) of Schedule 1 (The Services).
Onboarding	Implementation: • By Service Commencement: Provide a plan or confirmation of the onboarding arrangements. • By Service Commencement: Migrate 11 existing accounts to the Supplier environment, including making adjustments to 4 of the DWP accounts so that they follow the correct naming convention • On Service Commencement: Create 4 new accounts in the background and then transfer the users. These users will need to reactivate their credentials, but the Supplier will work with the relevant teams to ensure that any disruption is kept to a minimum.

Offboarding	Exit planning: • Within two weeks of Service Commencement: Provision of an Exit Plan of processes, timescales and costs for the deactivation and closure of accounts and other activities associated with exiting the Call-Off Contract.
Collaboration agreement	Not Used
Limit on Parties' liability	The annual total liability of either Party for all Property Defaults will not exceed £1,000,000. The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). 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. The annual total liability for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). Clause 24.1 in Part B below provides a definition of Other Defaults.

Insurance	The insurance(s) required will be: • Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law. • Employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law. All insurances required by this Call-Off Contract shall be maintained during the Call-Off Contract and for 6 years following the expiration or Ending of this Call-Off Contract.
Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 90 consecutive days.
Audit	The following Framework Agreement audit provisions are incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits: Clauses 7.4 to 7.13 of the Framework Agreement.
Buyer's responsibilities	• The Buyer is responsible for providing the Supplier with the applicable P2P general ledger account codes and category codes, so these can be included on applicable invoices in accordance with clause 8.1.5 of Schedule 1. • The Buyer agrees to use the data/materials received from the Supplier pursuant to the provision of the Services in accordance with all applicable Laws. • The Buyer agrees not to alter any copyright or other intellectual property right acknowledgement or confidentiality marking incorporated into or applied to the data/materials provided to it by the Supplier, pursuant to the provision of the Services.

	• The Buyer agrees not to reference the Supplier's Subcontractors (or any services provided by its Subcontractors) in any promotional materials. • Pursuant to paragraph 20 of Schedule 4 of the Framework, the Buyer before providing any Input Data to the Supplier or otherwise conducting a Search in relation to an individual consumer, shall: o notify the individual about whom a Search is made that their information will be disclosed to a credit reference agency, which may keep a record of that information and disclose it (and the fact that a search was made) to its other customers, including for the purposes of assessing the risk of giving credit and occasionally to prevent fraud, money laundering and to trace debtors; o make a copy of the CRAIN available to the individual so that they might understand how the credit reference agencies process their personal data; and o on request (which may be received directly or via the Supplier), provide a copy of the notification used to satisfy the above obligations to the individual concerned. • Where the Buyer is relying on an Exemption to process any Personal Data contained within any data supplied by the Buyer or Output Data: o The Buyer shall notify the Supplier in writing of the relevant Exemption relied on, providing details as to why the Exemption applies; o The Buyer warrants that it can rely on the Exemption in relation to its processing of such personal data; and o The Buyer shall immediately inform the Supplier should it no longer be able to rely on the Exemption.
Buyer's equipment	Not Used

Supplier's information

Subcontractors or partners	• BT Group • GB Group • DOW Jones Limited • BAE Systems • OCTA

Call-Off Contract charges and payment

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

Payment method	The payment method for this Call-Off Contract is Purchase Order by BACS.
Payment profile	As set out in Schedule 2.
Invoice details	The Supplier will issue one electronic invoice monthly in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	Electronic Invoices (attached to E-Mails) should be sent to: **APinvoices-DWP-U@gov.sscl.com(link sends e-mail)** Please note that with electronic invoices sent by email to SSCL, any covering message in the mail will be removed and **NOT** seen by the SSCL processing team. Other points to note are: • All files/invoices need to be in PDF format; • One PDF per invoice – all supporting documentation should be included within the single PDF; • Suppliers should not attach additional/separate supporting documentation as a separate file; • Multiple invoices can be attached to one email, **but** each invoice must be in a separate PDF (with no additional supporting files as described above).

	Invoicing enquiries should be sent to the assigned Operational Contract Manager in the first instance.
Invoice information required	All invoices must include the Invoicing Mandatory Information as set out in clause 8, (Payment and Invoicing) of Schedule 1 (The Services) of this Call-off agreement.
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	The total estimated value of this Call-Off Contract is £1,257,122.86 (+ VAT), based on estimated volumes. Actual volumes could be higher or lower than estimated, and no guarantee of volumes is made.
Call-Off Contract charges	The breakdown of the Charges is as per the Supplier's rate card as detailed in clause 1, Schedule 2 (Call Off Contract Charges) of this Call-off Contract.

Additional Buyer terms

Performance of the Service and Deliverables	• The Supplier must have completed all migration activity (specified in Schedule 1) before 21 September 2022. • The Services must be available for use by the Buyer from 21 September 2022.
Guarantee	In lieu of a requirement to provide a Guarantee, the Supplier agrees to include the following statement in its published audited annual accounts filed with the Registrar of Companies for England and Wales with respect to the period of 1 January 2021 to 31 December 2021, and to file such accounts with the Registrar of Companies by no later than 30 September 2022: "The company has also obtained a letter of parental support from Equifax Inc. the company's ultimate parent undertaking. Management are confident the company has adequate resources and parental support available as well as debt facilities in place to meet liabilities as they fall due."

	The Supplier shall promptly make a copy of those accounts available to the Buyer, and in any event within 24 hours of their publication.
Warranties, representations	Not Used
Supplemental requirements in addition to the Call-Off terms	• The Supplier will provide the Services and carry out its responsibilities under this Call-Off Contract in accordance with Schedule 1 and comply with the obligations specified in Schedule 1. • The Supplier will comply with and deliver the Services in accordance with the security requirements specified at clause 12 of Schedule 1 and comply with and deliver the Services in accordance with security requirements, standards and Buyer security policies specified in Schedule 8.
Alternative clauses	Not Used
Buyer specific amendments to/refinements of the Call-Off Contract terms	• Clause 2.1 of Part B: Terms and conditions of this Call-Off Contract is amended to also incorporate clauses 7.4 to 7.13 (Audits) of the Framework Agreement into this Call-Off Contract. • Clause 3.1 of Part B: Terms and Conditions shall be deleted and replaced by the following: 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. Supplier's Terms included as part of its Application (as embedded below).  453785448844410-terms-and-conditions- • Clause 16.1 of Part B: Terms and conditions of this Call-Off Contract is amended to provide that any security plans must comply with the Buyer's security

	policies, processes, requirements and standards specified in Schedule 8. • Clause 8.59 of the Framework as incorporated into Part B: Terms and conditions of this Call-Off Contract by virtue of clause 2.1, is hereby amended so the obligation to comply with Schedule 4 applies to both Parties. • Clause 18.1 of Part B: Terms and Conditions shall be deleted and replaced by the following: 18.1 Either Party can End this Call-Off Contract at any time by giving written notice to the other, as specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice. *Annex 1 – Product Rules* *The following Product Rules will apply to the provision of the Services.* *BT OSIS END USER TERMS/PRODUCT RULES* *These BT OSIS Terms shall only apply where the Buyer receives BT OSIS Data as part of the PSG Service.*

"BT"	*shall mean British Telecommunications plc;*
"BT OSIS Data"	*the name, address and telephone number of a consumer or busi*
"BT Marks"	*shall mean registered or unregistered trademarks and service marks and marks of ownership, trading names, brand names, dis schemes, devices, styles, emblems and other manifestations as BT;*
"You" or "Your"	*shall mean the Licensee's customer;*
"Licensee"	*shall mean Equifax Limited.*

- *For the purposes of these BT OSIS Terms, the following definitions shall apply:*
- *These BTOSIS Terms shall apply only to the extent that You receive BT OSIS Data from the Licensee.*
- *In relation to Your receipt and use of BT OSIS Data, You shall:*
    - *comply with all applicable laws and codes of practice including those in relation to data protection and privacy of information;*
    - *use all reasonable endeavours to prevent any unauthorised disclosure of any BT OSIS Data and keep it appropriately secure and confidential; and*
    - *only use or process any of BT OSIS Data for Your own internal purposes or, in the alternative, for a single use for a single specific person who is Your customer.*
- *To the extent that any complaint is made which relates to Your use of the Information, You shall assist BT and the Licensee in investigating the complaint and shall take such steps as are reasonably necessary to remedy the complaint as soon as practicable.*
- *You shall not:*

	○ *distribute, publish or display any material amount of the BT OSIS Data by any means, except as otherwise permitted by these BT OSIS Terms;* ○ *export or permit the export of the BT OSIS Data to a country which is not within the UK or European Economic Area, without the prior written express consent of the Licensee and/or BT;* ○ *have any rights to use the BT Marks and shall not make reference to BT or any BT product or service in any promotional or marketing advertising, communications, literature or packaging; and* ○ *alter any copyright or other intellectual property right acknowledgement or confidentiality marking incorporated into or applied to the BT OSIS Data and/or documentation owned by BT.* • *You acknowledge that BT OSIS Data only provides the surname of an individual and therefore does not, on its own, meet the full name match threshold outlined in the HM Treasure approved Joint Money Laundering Steering Group 'JMLSG' (AML industry) guidelines for use as part of anti-money laundering checks."* *Dow Jones End User terms apply if the Output Data being taken by the Buyer includes the Supplier's Equifax Watchlist product.* *The Buyer shall when using the Equifax Watchlist abide by the following End User Agreement terms;* *The terms set out in this End User Agreement ("EUA") apply to the Dow Jones Data, which shall be considered as Data for the purpose of the agreement between the Buyer and the Supplier relating to the supply Dow Jones Data by Equifax Limited ("Equifax") (the "Agreement"). Unless otherwise defined in EUA, any defined terms shall have the meanings given in the Agreement.* *In this EUA, the following terms shall have the following meanings:* *"Dow Jones Data" means personal data (full name, maiden name or AKAs, place and date of birth, country of residence and country of citizenship, occupation and information on additional roles and the relationship (if applicable) to a public figure) compiled and maintained by Dow Jones on data*

	subjects, including Politically Exposed Persons (PEPs) and Special Interest Persons (SIPs) which includes individuals due to his/her prominence in the news owing to his/her involvement in selected criminal activity: *"Dow Jones" means Factiva Limited, a company incorporated in England and Wales under number 3773253 and with registered address at The News Building, 1 London Bridge Street, SE1 9GF London, England, acting on behalf of Dow Jones & Company, Inc. and any of its affiliated companies; and* *"Permitted User" means an individual authorised to access and use the Dow Jones Data and who is either: (a) an individual employee of the Buyer; (b) an individual performing the functions of an employee on a temporary basis, independent contractor or consultant, in each case who is performing work for the Buyer; [or (c) an individual working for a company engaged by the Buyer ("Third Party Contractor") to perform research using the Dow Jones Data on the Buyer's behalf, for the benefit of the Buyer] provided that the Buyer: (i) assumes full responsibility and liability for the acts and omissions of all Permitted Users [and the Third Party Contractor], as if such acts and omissions were committed or made by the Buyer; and (ii) ensure that the Third Party Contractor and all Permitted Users use the passwords (provided by the Buyer) only on a dedicated basis for the Buyer.* • *Licence* o *The Supplier will supply the Dow Jones Data to the Buyer from the Start Date for the Dow Jones Data set out in the Buyer Agreement and grants to the Buyer a non-exclusive, non-transferable, non-sub licensable, non-assignable licence to use the Dow Jones Data subject to the terms and conditions of the Agreement and this EUA.* o *The Dow Jones Data contains information derived from publicly available sources, and will be regularly up-dated by the Supplier as updates are received from Dow Jones. Dow Jones retains control and ownership of the form and content of the Dow Jones Data, and although Dow Jones may alter the Dow Jones Data from time to time, its fundamental nature will not be changed. The Buyer and Permitted Users [and Third Party Contractor] will not, under the Agreement and this EUA acquire any ownership rights in the Dow Jones Data.*

- *Terms of use*
    - *The Buyer and Permitted User [and Third Party Contractor] shall use the Dow Jones Data in strict compliance with applicable laws and regulations within the jurisdictions in which it accesses and uses the Dow Jones Data. The Buyer shall ensure that the Dow Jones Data shall only: (a) be accessed by Permitted Users [and/or a Third Party Contractor]; and (b) be used for the legitimate interests of the Buyer and particularly for the purposes of assisting in complying with legal duties and regulations which apply to the Buyer such as due diligence, anti-money laundering, "know your customer" compliance or similar regulatory screening obligations.*
    - *Except to the extent permitted or required for the Buyer's permitted use under section 2.1, the Buyer and/or Permitted Users [and/or Third Party Contractor] shall not: (a) reproduce, distribute, display, sell, publish, broadcast or circulate the Dow Jones Data to any third party, nor make the Dow Jones Data available for any such use; or (b) create or store in electronic form any library or archive of the Dow Jones Data save that, and notwithstanding anything to the contrary, the Buyer shall be entitled to retain copies of the Dow Jones Data necessary for archival, regulatory and/or compliance purposes. The Buyer's right to retain such copies as set forth above shall survive termination/expiration of this EUA provided that it no longer actively uses the Dow Jones Data.*
    - *The parties agree that upon termination of the provision of the Dow Jones Data and unless otherwise provided by subject applicable legal or regulatory restrictions, the Buyer shall return or destroy all Dow Jones Data together with any copies, and certify in writing to the Supplier the completion of this process. In the case where the Buyer is required by law or regulation to keep copies of some of the Dow Jones Data, the Buyer guarantees the confidentiality of the Dow Jones Data and will not use the Dow Jones Data for any other purpose.*
- *Data Protection principles*
    - *The Buyer shall comply with all applicable laws and regulations within the jurisdictions, in which the Buyer processes the Dow Jones Data, and the Data Processing Principles set out below.*

	The Buyer acknowledges that an individual who is included in the Dow Jones Data (an "Individual") can enforce in his/her country of establishment this provision against the Buyer with respect to its personal data. Any person acting under the authority of the Buyer, including a data processor, shall be obligated to process the Dow Jones Data only on instructions from the Buyer and on terms no less stringent than those set out in the Data Processing Principles below. o *Upon reasonable request of the Supplier, the Buyer will submit its data processing facilities, data files and documentation needed for processing to review, audit and/or certification by the Supplier (or any independent or impartial inspection agents or auditors, selected by the Supplier and not unreasonably objected to by the Buyer) to ascertain compliance with the warranties and undertakings in this EUA, with reasonable notice and during regular business hours. Such request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Buyer, which consent or approval the Buyer will attempt to obtain in a timely fashion.* • *Warranties* *The Supplier shall make reasonable efforts to ensure that the Dow Jones Data is up to date. While the Supplier will use its reasonable efforts to ensure that the Dow Jones Data is complete, the Supplier cannot warrant that the Dow Jones Data includes a complete or accurate archive of every public figure or their associates in each country. Except as specified in this EUA all express or implied representations, warranties, conditions and undertakings in relation to the provision of the Dow Jones Data are excluded.* • *Buyer Information* *Please note that the Supplier will report to Dow Jones the name of the Buyer and the number of name queries screened against the Dow Jones Data, but not its nature. This information will only be used by Dow Jones to verify the relevant usage of the Dow Jones Data and the payments due and payable to Dow Jones in this respect. Dow Jones shall not disclose such information to any third party, other than to members of its group companies, or use them for any other purpose whatsoever and will treat this information as Confidential Information.*

	DATA PROTECTION PRINCIPLES *1. Purpose limitation: Personal Data may be processed and subsequently used or further communicated only for the following purposes: (a) assisting in complying with legal duties and regulations which apply to the Subscriber Group; (b) performing a statutory role as a Governmental organization; or (c) performing law enforcement duties. If the Subscriber or a member of the Subscriber Group is processing special categories of data, defined under Article 8 of the European Directive 95/46/EC as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life ("Sensitive Data"), it shall only process it for the purpose of preventing fraud or a similar crime (the "Purposes").* *2. Personal Data quality and proportionality: Personal Data must be accurate and, where necessary, kept up to date. Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.* *3. Transparency: Individuals must be provided with information necessary to ensure fair processing (such as information about the purposes for processing and about the transfer), unless such information has already been given by the Supplier.* *4. Security and confidentiality: Technical and organisational security measures must be taken by the Buyer that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. This obligation shall not apply where the Buyer is accessing services via the hosted solutions of the Supplier.* *5. Rights of access, rectification, deletion and objection: An Individual must, whether directly or via a third party, be provided with the Dow Jones Data about him/her that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or have been dismissed by the relevant data protection authorities, or when doing so would be likely to seriously harm the interests of the Buyer or other organisations dealing with the Buyer and such interests are not overridden by the interests for fundamental rights and freedoms of the Individual. The sources of the Dow Jones*

	Data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the Individual would be violated. An Individual must be able to have the Dow Jones Data about him/her rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the Supplier or the Buyer may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the Dow Jones Data has been disclosed need not be made when this involves a disproportionate effort. The burden of proof for any refusal rests on the Buyer or the Supplier, and the Individual may always challenge a refusal before the relevant data protection authorities. *6. Sensitive Data: The Buyer shall take such additional measures (e.g. relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under the Agreement or this EUA.*
	7. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the Supplier or the Buyer which produces legal effects concerning an Individual or significantly affects an Individual and which is based solely on automated processing of Dow Jones Data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, creditworthiness, reliability, conduct, etc. The Buyer shall not make any automated decisions concerning Individuals, except when: (a) (i) such decisions are made by the Buyer in entering into or performing a contract with the Individual, and (ii) the Individual is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties; or (b) where otherwise provided by applicable laws or regulations.
Public Services Network (PSN)	Not Used
Personal Data and Data Subjects	See Annex 1 of Schedule 7

1. Formation of contract

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

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

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

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

2. Background to the agreement

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

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

Signed	Supplier	Buyer
Name	James Atkin [**Enter name**]	Angela Smith [**Enter name**]
Title	General Counsel - Europe [**Enter title**]	Commercial Manager DWP [**Enter title**]
Signature	James Atkin James Atkin (Sep 20, 2022 17:04 GMT+1)	Angela Smith Angela Smith (Sep 20, 2022 17:07 GMT+1)
Date	20-Sep-2022 [**Enter date**]	20-Sep-2022 [**Enter date**]

Schedule 1: The Services

1. Credit Reference Agency Services

1.1 The Supplier is required to provide access, via a secure web-based online portal or integrated Application Programming Interface (API) service, to a range of information, based on multiple sources of data, including Credit Reference Agency (CRA) data. Agent* input of agreed Customer** details will generate reports containing information that is both relevant and proportionate to the enquiry.

1.2 There may be a need to obtain indications of residency, to verify and enhance existing Customer data, or to assess ability to pay via automated assessment and validation of personal financial circumstances, including the completion and validation of personal income and expenditure.

1.3 The service will support the negotiation and agreement of sustainable payment plans for the recovery of overpaid benefit or child maintenance arrears. It will also support fraud investigations and, where necessary, decisions to instigate court prosecutions.

**Agent(s): Person(s) acting on behalf of the Buyer, including third party supplier operators.*

*** Customer: A person who is or has been in Debt to the Buyer.*

2. Background and Context

2.1 The Department for Work and Pensions is a major Government Department responsible for welfare, pensions and child maintenance policy. As the UK's biggest public service department it administers the State Pension and a range of working age, disability and ill health benefits to around 20 million claimants and customers.

2.2 Not used.

2.3 The Buyer is a ministerial department, supported by 13 agencies and public bodies. The Buyer provides services in several ways, for example through Jobcentre Plus, The Pension Service, the Child Maintenance Service and partner organisations. More information on the Buyer's work and overall objective is available in the following links to our Gov.UK website and our Outcome Delivery Plan 2021-22:

- https: //www.gov.uk/government/organisations/department-for-work-pensions/about
- https: //www.gov.uk/government/publications/department-for-work-and-pensions-outcome-delivery-plan

2.4 The Buyer's Debt Management Team specialises in the management and recovery of funds owed to government using a range of debt management and recovery strategies, including outsourced Debt collection.

2.5 The Buyer's Counter Fraud and Compliance Team specialises in the identification and prevention of fraud. This protects the welfare budget from those who would seek to abuse it.

2.6 The Debt Management and Counter Fraud and Compliance Teams within the Department for Communities (DfC) have similar specialisms.

2.7 Teams within the Buyer's Child Maintenance Group specialise in the recovery of child maintenance arrears from non-compliant, non-resident parents for redirection to relevant vulnerable families and children who need it.

2.8 Use of CRA Services, within both the Buyer and DfC, supports internal recovery methods and fraud identification activities.

2.9 The requirement for CRA Services has arisen due to the forthcoming expiry of the Buyer's existing Agreement on 20/09/2022. Replacement services are therefore required.

2.10 The Buyer aims to award a new agreement for commencement no later than 21/09/2022. A smooth transition of services is required to reduce any Disruption to delivery.

3. The Requirement

3.1 Online Service

3.1.1 The Buyer requires a secure, online service / web-based portal with a user-friendly and intuitive interface. Upon log in, Agents will require instant access to the online service.

3.1.2 Agent input of agreed Customer details will generate focused and formatted reports containing information that is both relevant and proportionate to the enquiry, such as:

- Tracing the Customer;
- Verifying and enhancing data relating to the Customer;
- Informing an appropriate Collection Strategy, or;
- Informing payment negotiations with the Customer.

3.1.3 The reports must include:

- An affordability measure, financial status and address data;
- Property insight data, including estimated equity amount;
- The most recent mobile and land line phone numbers, where available.

3.1.4 The Buyer requires the Supplier to set up user roles with separate permissions, as follows:

- Administrator Role – able to create, suspend, remove and view all user reports/searches;
- Team Leader / Operator Role – able to view only access of clerical operator searches;
- Clerical Operator – able to use the search facility and view reports.

3.1.5 The Administrator Role must be able to create teams and assign users to teams. The Administrator Role must be able to extract the following:

- Agent MI;
- Active and inactive accounts;
- Date of creation;
- Date of last login.

3.2 Integrated API Service

3.2.1 The Buyer requires a secure, integrated service through an API direct to Child Maintenance Service (CMS) systems.

3.2.2 On input of agreed details, all information required should be integrated into CMS Systems, including information that is both relevant and proportionate to the need, such as:

- Tracing the Customer;
- Verifying and enhancing data relating to the Customer;
- Informing an appropriate Collection Strategy, or;
- Informing payment negotiations with the Customer.

3.2.3 The integrated service must provide:

- An affordability measure, financial status and address data;
- Property insight data, including estimated equity amount;
- The most recent mobile and land line phone numbers, where available.

3.3 Both Online and Integrated API Service

3.3.1 Both the online and integrated API service must be able to be accessed via a multitude of platforms. Microsoft Edge browser is currently used for this purpose.

3.3.2 Accessing an individual's information should not leave a footprint on the individual's account.

3.3.3 The service must provide an Agent timeout notification.

3.3.4 The Supplier shall provide user training including all training materials.

3.3.5 Supplier must provide weekly individual user usage reports to the nominated Buyer contact in an excel format via the approved secure method.

3.4 Data and Volume Forecasts

3.4.1 Bespoke report requirements can be categorised as described in Table 1. below. It should be noted that volumes are subject to fluctuation and not guaranteed.

Table 1: Report Requirements and Forecast Volumes

Report Category	Description	Report Types	Volumes
FIND	Data enabling the location of an individual.	Search	267,878
		Residency / Trace	240,698
		Phone Data	11,543
VERIFY	Data verifying an individual's personal and financial circumstances.	Debt Management	1,146,559
INVESTIGATE	Data providing a complete picture of an individual or business, including financial status.	Investigation	11,000
		Commercial Data	200
Total			1,677,878

4. Accessibility

4.1 The Supplier must provide evidence that their products and services on offer shall meet Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and therefore the products and/or services will:

- Meet level AA of the Web Content Accessibility Guidelines (WCAG 2.1) as a minimum;
- Work on the most 'commonly used' assistive technologies, including screen magnifiers, screen readers and speech recognition tools;

- Confirm that a valid proportion of disabled people will be used in user research;
- Provide an accessibility statement explaining how accessible the service will be and publish this when the service moves into the public domain.

5. Service Availability

5.1 The Buyer's contracted working hours are 08:00 hours to 20:00 hours Monday to Friday and 09:00 hours to 16:00 hours on Saturday. As such, the services must be available during these time periods.

5.2 Technical support services in the event of unplanned downtime, access or administration issues and IT security breaches, are required for exceptions, including evenings, weekends and bank holidays.

5. 3 The Supplier is required to have the resources and solutions to flexibly meet these requirements to support the Buyer during the course of its business.

6. Key Milestones and Deliverables

6.1 Key milestones and deliverables that are critical to the fulfilment of the Contract are specified in the Order Form and Table 2. below.

6.2 All documentation should be provided in electronic format compatible with Microsoft Office 365 or PDF and signed and dated by the relevant Supplier key personnel.

.

Table 2. Key Milestones and Deliverables

Milestone	Requirement / Provision of:	Timeframe for Delivery
1	Implementation: • By Service Commencement: Provide a plan or confirmation of the onboarding arrangements. • The migration of 11 existing accounts to the Supplier environment, including making adjustments to 4 of the DWP accounts so that they follow the correct naming convention.	By Service Commencement.
2	Implementation: • The creation of 4 new accounts in the background and then transfer the users. These users will need to reactivate their credentials, but the Supplier will work with the relevant teams to ensure that any disruption is kept to a minimum.	On Service Commencement
3	• Key personnel / teams contact details, and • Detailed standard operating procedures for complaints, issues resolution and escalation.	Within two weeks of Service Commencement.
4	Exit Planning: • Provision of an Exit Plan of processes, timescales and costs for the deactivation and closure of accounts and other activities associated with exiting the Call-Off Contract.	Within two weeks of Service Commencement.

7. Management Information / Reporting

7.1 Minimum Expectations

7.1.1 The Supplier must be able to provide all Management Information (MI) and reporting in formats that are compatible with Microsoft Office 365, e.g. Microsoft Excel via electronic means.

7.1.2 The Supplier should only use PDF format for the provision of contextual documentation to support the analysis of MI.

7.1.3 In the event the Supplier is unable to provide an electronic reporting system, the Buyer can provide access to its own eTendering system ‘Jaggaer’, which enables electronic file sharing between Suppliers and the Buyer.

7.1.4 The Supplier must ensure to supply a definitions list for all abbreviations utilised in MI and reporting.

7.1.5 The Supplier must not amend format or fields of MI without prior notice in writing to the Buyer.

7.2 Detailed MI Reporting

7.2.1 The Supplier must ensure the accurate and timely provision of a detailed single MI report no later than the 7th working day of the following month, in line with the Buyer's internal reporting deadlines.

7.2.2 The Supplier is required to provide detailed MI as close to 'real time' as possible to support the Buyer's internal reporting and financial systems. MI must be provided monthly as the minimum frequency requirement as detailed in the table below.

7.2.3 The Supplier must ensure the detailed MI shows the breakdown of all charges at the month-end position i.e. covering a full calendar month.

7.3 Performance Reporting

7.3.1 The Supplier must provide monthly performance reports against the to-be-agreed Service Level Agreements (SLAs) no later than the 7th working day of the following month. The Supplier must also detail the calculation of any Service Credit due against each SLA.

7.4 Freedom of Information Requests (FOIs) and Parliamentary Questions (PQs)

7.4.1 The Buyer may request ad hoc MI from the Supplier to support individual data requests as relates to Freedom of Information requests and Parliamentary Questions.

7.4.2 Due to the nature of these requests, the deadlines may vary and will be communicated to and agreed with the Supplier in writing at the point of the request.

7.5 Summary of Reporting Requirements

7.5.1 Summarised reporting requirements are detailed in Table 3. below.

Table 3. Summary of Reporting Requirements

Ref	Report	Frequency
1	Detailed MI report capturing the following information: • Staff name; • Staff location; • Staff email address or User ID; • Date and time the search/trace was performed; • Customer reference; • Customer name; • Customer address; • Report type generated.	Monthly, no later than the 7th working day of the following month.
2	User Activity Report capturing the following information: • Staff location; • Staff email address or User ID; • Active/inactive status; • Date last logged in.	Monthly, no later than the 7th working day of the following month.
3	Summary MI report, year-to-date view of report usage levels.	Monthly, no later than the 7th working day of the following month.
4	Performance report against SLAs including any Service Credit calculation.	Monthly, no later than the 7th working day of the following month.
5	FOIs and PQs.	Ad hoc, within agreed deadlines.

8. Payment and Invoicing

8.1 Payment and Invoicing Mechanism(s)

8.1.1 The Supplier must be prepared to use electronic Purchase to Pay (P2P) routes, including payment by purchase order and e-Invoicing.

8.1.2 The Supplier must be prepared to work with the Buyer to set up and test all electronic P2P routes. This may involve creating technical ordering and invoice files, including working with our Enterprise Resource Planning (ERP) system service suppliers and systems.

8.1.3 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

8.1.4 Before Payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

8.1.5 The Supplier must ensure all mandatory fields meet the required format as detailed in Table 4. below.

Table 4. Invoicing Mandatory Information

Data Required	Data Format	Invoicing Mandatory Information
Invoice reference	Text / General	✓
Invoice date	Date	✓
Invoice breakdown	Text	✓
Invoice breakdown	Currency	✓
Invoice net value	Currency	✓
Invoice VAT	Currency	✓
Invoice VAT status	Text	✓
Invoice total value	Currency	✓
Buyer P2P general ledger account code and category code (to be provided by the Buyer)	Text	✓

8.2 Invoicing Requirements and Schedule

8.2.1 The Buyer will provide all address and contact details for invoicing and related queries or escalations, during the implementation phase of the Contract.

8.2.2 The invoicing schedule will be monthly in arrears.

9. Continuous Improvement

9.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

9.2 The Supplier should present opportunities and recommendations for Continuous Improvement to the Buyer during Contract review meetings.

9.3 Change to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed in writing prior to any changes being implemented.

10. Staff and Customer Service

10.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract to consistently deliver a quality service.

10.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

10.3 The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

11. Service Levels and Performance

11.1 The Buyer will use Key Performance Indicators (KPIs) to measure the quality of the Supplier's delivery as detailed in Table 5. below.

Table 5. Key Performance Indicators

KPI	Service Area	KPI Description	Measurement Period	Target	Severity Level		
					Minor	Material	Critical
1	Security	The Supplier shall report a Breach of Security to the nominated Buyer Representative through the incident reporting process immediately and no later than 12 hours (24/7) after discovery.	Monthly Number of Breaches of Security not reported within 12 hours of discovery.	All	One failure	More than one but less than 3 failures	3 or more failures
2	Service Availability	The Online Service and Integrated API Service will be available between the hours of 08:00-20:00 Monday to Friday and 09.00-16.00 on Saturday.	30 Rolling Days % time Online Service and Integrated API Service is available in the specified hours, over the Measurement Period.	98%	Is 95% or higher but less than 98%	Is 85% or higher but less than 95%	Is less than 85%

12. Security Requirements

12.1 Security and Audit

12.1.1 The Supplier shall hold an FCA license with the required permissions to operate this service.

12.1.2 The Supplier shall comply with requests for information from the Independent Case Examiner (ICE), the Buyer Parliamentary Business Unit (PBU), System Access Requests (SARs) and those requests stimulated by PQs, FoIs and any other ad hoc requests for information by specified timescales. These requests are to be managed in accordance with Buyer security rules in respect of the transfer of data.

12.1.3 The Supplier shall be required to demonstrate updated detailed business continuity and disaster recovery plans. These plans must be in place in readiness for Day 1 commencement.

12.2 IT Security Standards

12.2.1 The Supplier shall ensure sufficient resilience on their systems and infrastructure deployed to connect to and receive/transfer information to the Buyer's infrastructure in line with contractual agreements.

12.2.2 The Supplier must provide a support/service desk for the logging of incidents during the Agreed Service Time. All contact with the supplier support/service desk must be logged and reported on.

12.2.3 Incident reports should be provided for all Priority 1 and 2 incidents detailing the cause of the incident, impact, resolution and any mitigating actions taken.

13 Implementation

13.1 All implementation must be robust and agreed with the Buyer and shall not be considered complete until this has been confirmed by the Buyer.

13.2 The Service must be available in full from 21/09/2022 (Service Commencement).

14 Contract Management

14.1 The Buyer – what you can expect from us:

14.1.1 The Buyer will provide a designated contact as an Operational Contract Manager (OCM) to manage the day-to-day running of the contract and performance monitoring activity.

14.1.2 The Buyer will provide a designated contact as a Commercial Contract Manager to manage key Contractual activity including but not limited to:

14.1.3 Contract Variations including amendments to Contract documentation, addition/removal of service lines, extensions or uplifts to Contract value;

- Pricing reviews;
- Estimate usage reviews;

14.1.4 The Buyer will provide a definitive list of contacts for specific requirements of the contract during the implementation period, e.g. Digital or Security, in the event of queries.

14.1.5 The Buyer OCM will attend all review meetings.

14.1.6 The Buyer may invite key internal stakeholders to review meetings to support specific contract and performance management-related activities, or continuous improvement projects.

14.2 Supplier Personnel

14.2.1 The Supplier must provide a designated contact as the responsible Account Manager to The Buyer.

14.2.2 The Supplier's designated Account Manager must be an experienced senior manager who can work with the Buyer to provide strategic leadership and input, and in particular management of the Services, including attendance at all review meetings.

14.2.3 In the event of sub-contracting arrangements, the Supplier's designated Account Manager will have responsibility for ensuring the attendance of key delivery partners where required at review meetings.

14.2.4 The Supplier is expected to provide a list of key personnel who will be involved in the delivery of the services for this Agreement and contact details within two (2) weeks of contract Award.

14.3 Review Meetings

14.3.1 Monthly and/or Quarterly Business Review Meetings will be led by the Buyer to discuss operational performance achievement, with facilitation and secretariat provided by the Supplier.

14.3.2 Annual review meetings facilitated by the Supplier to include Security, Compliance and Financial reviews as agreed in advance with the Buyer

14.3.3 Meetings may be conducted virtually via MS Teams, or in person.

14.3.4 Attendance at review meetings held at the Buyer's premises shall be attended at the Supplier's own expense.

14.3.5 The Supplier is expected to provide electronic copies of all appropriate MI and a summary of complaints and issues for the relevant period at review meetings.

14.3.6 Monthly and/or Quarterly Business Review Meetings will be led by the Buyer to discuss operational performance achievement, with facilitation and secretariat provided by the Supplier.

14.3.7 Annual review meetings facilitated by the Supplier to include Security, Compliance and Financial reviews as agreed in advance with the Buyer.

Schedule 2: Call-Off Contract Charges

1. Call-Off Contract Charges

1.1 The detailed Charges breakdown for the provision of Services is as detailed in Table 6. and Table 7. below:

Table 6. Equifax Ltd. Public Sector Gateway Service: Rate Card

Equifax Online portal Checks Rate Card.xlsx

Table 7. Applicable Price Per Report

Report Type	Price Per Report
Advanced Searching	0.154
Debt Management Report	0.893
Enhanced Phone Data	0.143
Full-Investigation Report	3.325
Residency Check	0.639
Trace Person	0.639
Commercial Data	2.55

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)
- 7.4 to 7.13 (Audits)
- 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 policies, processes, requirements and standards specified in Schedule 8, and protect all aspects and processes associated with the delivery of the Services.

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

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

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

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

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

21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

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

24. Liability

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

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

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

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common

law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

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

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

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

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

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

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

29.6.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

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

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

32. Variation process

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

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

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

33. Data Protection Legislation (GDPR)

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

Schedule 3: Collaboration Agreement

1. Not Used

Schedule 4: Alternative clauses

1. Not Used

Schedule 5: Guarantee – Not Used

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: • information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above • other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
CRAIN	means the Credit Reference Agency (CRA) Information Notice, the industry standard privacy information policy adopted by the leading UK CRAs (a copy of which can be found here:

	https://www.equifax.co.uk/crain), and as may be updated from time to time;
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)

DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Exemptions	means any exemptions under the Data Protection Act 2018 or other Data Protection Legislation, which exempt the requirement to provide fair notice to data subjects in relation to the processing of their Personal Data;
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available The following do not constitute a Force Majeure event: • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those

	services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	Can be: • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand

	• a Schedule A1 moratorium
Intellectual Property Rights or IPR	Intellectual Property Rights are: • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: • the supplier's own limited company • a service or a personal service company • a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).
IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.

Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.

Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Output Data	means any information or data provided by the Supplier and received by the Buyer pursuant to the Services;
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.
Product Rules	Means those additional terms and conditions set out in the Order Form ;

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:
	• induce that person to perform improperly a relevant function or activity
	• reward that person for improper performance of a relevant function or activity
	• commit any offence:
	  ○ under the Bribery Act 2010
	  ○ under legislation creating offences concerning Fraud
	  ○ at common Law concerning Fraud
	  ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.

Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Search	means a search made by a Buyer of the Supplier's database (including via the Supplier) for the purpose of obtaining information in relation to an individual or corporate entity;
Services	The services ordered by the Buyer as set out in the Order Form.

Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.

Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

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

Annex 1: Processing Personal Data

1.1 The contact details of the Buyer's Data Protection Officer are:

Dominic Hartley
DWP Data Protection Team
Benton Park View 6
Room BP6001
Mail Handling Site A
Wolverhampton
WV98 1ZX

data.protectionofficer@dwp.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are: Adrian Leung, 1. Angel Court, London, EC2R 7HJ, Adrian.Leung@equifax.com

Descriptions	**Details**
Identity of Controller for each Category of Personal Data	**The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● Business contact details of Supplier Staff for which the Supplier is the Controller ● Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller ● All other Personal Data received pursuant to Services
Duration of the Processing	21/09/2022 to 20/09/2023
Nature and purposes of *the* Processing	

	The Supplier is required to provide access, via a secure web-based online portal or integrated Application Programming Interface (API) service, to a range of information, based on multiple sources of data, including Credit Reference Agency (CRA) data. Agent* input of agreed Customer** details will generate reports containing information that is both relevant and proportionate to the enquiry. There may be a need to obtain indications of residency, to verify and enhance existing Customer data, or to assess ability to pay via automated assessment and validation of personal financial circumstances, including the completion and validation of personal income and expenditure. The service will support the negotiation and agreement of sustainable payment plans for the recovery of overpaid benefit or child maintenance arrears. It will also support fraud investigations and, where necessary, decisions to instigate court prosecutions. The Parties agree that the Personal Data received pursuant to the delivery of the Services (excluding Personal Data received with respect to the administration of this Call-Off Contract) will only be used for the following purposes (unless use for another purpose is permitted by applicable Data Protection Legislation): • Detecting and preventing fraud - Identifying individual consumers or businesses making potentially fraudulent applications for credit and directly related Financial Services. Including undertaking (as applicable) address and bank account verification, employment status (and employer) checks, and Politically Exposed Person checks. In the context of this definition, “Fraudulent” means “fraud” as defined by the Fraud Act 2006 and any regulation, code of practice or government guidance (as amended or replaced from time to time). • Preventing money laundering and/or complying with legal obligations in relation to money laundering - Identifying transactions and patterns

	of behaviour within individuals or businesses that seek to conceal the origins of illegally obtained money, typically by means of money transfers involving foreign banks or legitimate businesses as more specifically defined by the Proceeds of Crime Act 2002 and any regulation, code of practice or government guidance (as amended or replaced from time to time). • Debt management and collection – Tracing the location and/or contact details of debtors and assessing their ability to repay outstanding debts using a variety of legally available debt collection methods. The above processing is necessary for the function of a government department and necessary for the purposes of employment, social security and social protection. The nature of the Processing includes all of the following: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. **Agent(s): Person(s) acting on behalf of the Buyer, including third party supplier operators.* *** Customer: A person who is or has been in Debt to the Buyer.*
Type of Personal Data	• Account Data - open /closed financial accounts, credit information. • Account Data, all financial institutions to include banking, mortgages, loans, credit cards • Alias Data • Anonymised Accounts (Insight data) showing name of financial company, account type, account numbers, date of opening / settlement / default, current balance, monthly account performance. • Associate Data • Bank account data – account and sort code numbers for accounts and credit card details and start dates, active and default accounts • Bankruptcy / sequestration information • Businesses at Postcode

	• CIFAS Data • Credit facility information, e.g. overdraft, mortgage, loan etc including account details and balance • Contact telephone numbers • Correspondence Address • Court & Insolvency Data • County Court Judgements • Credit facility information, e.g. overdraft, mortgage, loan etc including account details and balance • Date of Birth • Debit and Credit Card Details • Deceased Data • Details of applications for finance (e.g. bank details) used when applying for a loan. • Details of other debt payment arrangements in place Director information (incl. Directors Match Data and Directors Data at Postcode) • Directors Data at Postcode • Electoral Roll / Register data – current and previous residents of address plus customer previous addresses • Email Addresses • Employment status and details • Financial institutions used for credit application, whether defaulted or not • Financial status • Gender • Individual names (title, surname, forename, middle name) • Mortgage details • National Insurance Number • Notice of Correction • Open account information • Property Data including valuation • Residential address • Sanctions Data • Savings accounts details • Trace Adress Data • Telephone Data Personal details including name and contact details of Supplier Staff and those acting for the Buyer.
Categories of Data Subject	Customers who are, or have been, in debt to the Buyer, and non-resident parents who are, or have been, in arrears in respect of their obligation to pay child maintenance, via the Buyer, to the parent with care.

	Supplier Staff
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	Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under this Call-Off Contract, unless further retention or processing is permitted by applicable Data Protection Legislation.

Schedule 8: Enhanced Security Requirements

GENERAL

The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, comply with the Buyer's security requirements as set out in the Call-Off Contract which include the requirements set out in this Schedule 8 to the Call-Off Contract (the "**Buyer's Security Requirements**"). The Buyer's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Buyer assets, the Buyer's Systems Environment and the Supplier's Systems Environment.

Terms used in this Schedule 8, which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this Schedule 9, the following definitions shall apply:

"**Buyer Personnel**"	shall mean all persons employed by the Buyer including directors, officers, employees together with the Buyer's servants, agents, consultants, contractors and suppliers but excluding the Supplier and any Subcontractor (as applicable).
"**Availability Test**"	shall mean the activities performed by the Supplier to confirm the availability of any or all components of any relevant ICT system as specified by the Buyer.
"**CHECK**"	shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.
"**Cloud**"	shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.
"**Cyber Security Information Sharing Partnership**" or "**CiSP**"	shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.

"**Good Security Practice**"	shall mean: a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology); b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.
"**Information Security**"	shall mean: a) the protection and preservation of: i) the confidentiality, integrity and availability of any Buyer assets, the Buyer's Systems Environment (or any part thereof) and the Supplier's Systems Environment (or any part thereof); ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and b) compliance with all Law applicable to the processing, transmission, storage and disposal of Buyer assets. c)
"**Information Security Manager**"	shall mean the person appointed by the Supplier with the appropriate experience, authority and expertise to ensure that the Supplier complies with the Buyer's Security Requirements.

"**Information Security Management System ("ISMS")**"	shall mean the set of policies, processes and systems designed, implemented and maintained by the Supplier to manage Information Security Risk as certified by ISO/IEC 27001.
"**Information Security Questionnaire**"	shall mean the Buyer's set of questions used to audit and on an ongoing basis assure the Supplier's compliance with the Buyer's Security Requirements.
"**Information Security Risk**"	shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.
ISAE 3402	shall mean the International Standard on Assurance Engagements No. 3402 (ISAE) as most recently published by the International Auditing and Assurance Standards Board or its successor entity ("**IAASB**") or the relevant successor or replacement standard which is formally recommended by the IAASB.
"**ISO/IEC 27001, ISO/IEC 27002 and ISO 22301**	shall mean: a) ISO/IEC 27001; b) ISO/IEC 27002/IEC; and c) ISO 22301 in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO.
"**NCSC**"	shall mean the National Cyber Security Centre or its successor entity (where applicable).
"**Penetration Test**"	shall mean a simulated attack on any Buyer assets, the Buyer's Systems Environment (or any part thereof) or the Supplier's Systems Environment (or any part thereof).
"**PCI DSS**"	shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "**PCI**").
"**Risk Profile**"	shall mean a description of any set of risks. The set of risks can contain those that relate to a

	whole organisation, part of an organisation or as otherwise applicable.
"**Security Test"**	shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.
"**Tigerscheme**"	shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.
"**Vulnerability Scan**"	shall mean an ongoing activity to identify any potential vulnerability in any Buyer assets, the Buyer's Systems Environment (or any part thereof) or the Supplier's Systems Environment (or any part thereof).

1.2 Reference to any notice to be provided by the Supplier to the Buyer shall be construed as a notice to be provided by the Supplier to the Buyer's Representative.

2. PRINCIPLES OF SECURITY

2.1 The Supplier shall at all times comply with the Buyer's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE, CERTIFICATION AND AUDIT

3.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, obtain and maintain certification to ISO/IEC 27001 (the "**ISO Certificate**") in relation to the Services during the Call-Off Contract. The ISO Certificate shall be provided by the Supplier to the Buyer on the dates as agreed by the Parties.

3.2 The Supplier shall appoint:

a) an Information Security Manager; and

b) a deputy Information Security Manager who shall have the appropriate experience, authority and expertise to deputise for the Information Security Manager when s/he is on leave or unavailable for any period of time.

The Supplier shall notify the Buyer of the identity of the Information Security Manager on the Start Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Supplier shall ensure that it operates and maintains the Information Security Management System during the Call-Off Contract and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Call-Off Contract);

b) a risk assessment (which shall include any risks specific to the Services);

c) a statement of applicability;

d) a risk treatment plan; and

e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Supplier shall provide the Information Security Management System to the Buyer upon request within 10 Working Days from such request.

3.4 The Supplier shall notify the Buyer of any failure to obtain an ISO Certificate or a revocation of an ISO Certificate within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required in order to obtain an ISO Certificate following such failure or revocation and provide such ISO Certificate within one calendar month of the initial notification of failure or revocation to the Buyer or on a date agreed by the Parties. For the avoidance of doubt, any failure to obtain and/or maintain an ISO Certificate during the Contract Period after the first date on which the Supplier was required to provide the ISO Certificate in accordance with paragraph 3.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, obtain and maintain certification to ISO/IEC 27001 (the "**ISO Certificate**") in relation to the Services during the Call-Off Contract. The ISO Certificate shall be provided by the Supplier to the Buyer on the dates as agreed by the Parties. (regardless of whether such failure is capable of remedy) shall constitute a Material Breach.

3.5 The Supplier shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Buyer.

3.6 Notwithstanding the provisions of paragraph 3.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, obtain and maintain certification to ISO/IEC 27001 (the "**ISO Certificate**") in relation to the Services during the Call-Off Contract. The ISO Certificate shall be provided by the Supplier to the Buyer on the dates as agreed by the Parties. to paragraph 3.5 The Supplier shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Buyer., the Buyer may, in its absolute discretion, notify the Supplier that it is not in compliance with the Buyer's Security Requirements and provide details of such non-compliance. The Supplier shall, at its own expense, undertake those actions required in order to comply with the Buyer's Security Requirements within one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Buyer's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Material Breach.

4. RISK MANAGEMENT

4.1 The Supplier shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Call-Off Contract which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Buyer's Security Requirements are met (the **Risk Assessment**). The Supplier shall provide the Risk Management Policy to the Buyer upon request within 10 Working Days of such request. The Buyer may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Buyer's Security Requirements. The Supplier shall, at its own expense, undertake those actions required in order to implement the changes required by the Buyer within one calendar month of such request or on a date as agreed by the Parties.

4.2 The Supplier shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Supplier's Systems Environment or in the threat landscape or (iii) at the request of the Buyer. The Supplier shall provide the report of the Risk Assessment to the Buyer, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Supplier shall notify the Buyer within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

4.3 If the Buyer decides, at its absolute discretion, that any Risk Assessment does not meet the Buyer's Security Requirements, the Supplier shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

4.4 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, co-operate with the Buyer in relation to the Buyer's own risk management processes regarding the Services.

4.5 For the avoidance of doubt, the Supplier shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph **4. RISK MANAGEMENT**. Any failure by the Supplier to comply with any requirement of this paragraph **4. RISK MANAGEMENT** (regardless of whether such failure is capable of remedy), shall constitute a Material Breach.

5. SECURITY AUDIT AND ASSURANCE

5.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Buyer (the "**Information Security Questionnaire**") at least annually or at the request by the Buyer. The Supplier shall provide the completed Information Security Questionnaire to the Buyer within one calendar month from the date of request.

5.2 The Supplier shall conduct Security Tests to assess the Information Security of the Supplier's Systems Environment and, if requested, the Buyer's Systems Environment. In relation to such Security Tests, the Supplier shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material

change in the Supplier's Systems Environment or in the Buyer's System Environment or (iii) at the request of the Buyer which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Buyer. The Supplier shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Supplier shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Buyer in its absolute discretion.

5.3 The Buyer shall be entitled to send the Buyer's Representative to witness the conduct of any Security Test. The Supplier shall provide to the Buyer notice of any Security Test at least one month prior to the relevant Security Test.

5.4 Where the Supplier provides code development services to the Buyer, the Supplier shall comply with the Buyer's Security Requirements in respect of code development within the Supplier's Systems Environment and the Buyer's Systems Environment.

5.5 Where the Supplier provides software development services, the Supplier shall comply with the code development practices specified in the Specification or in the Buyer's Security Requirements.

5.6 The Buyer, or an agent appointed by it, may undertake Security Tests in respect of the Supplier's Systems Environment after providing advance notice to the Supplier. If any Security Test identifies any non-compliance with the Buyer's Security Requirements, the Supplier shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Buyer at its absolute discretion. The Supplier shall provide all such co-operation and assistance in relation to any Security Test conducted by the Buyer as the Buyer may reasonably require.

5.7 The Buyer shall schedule regular security governance review meetings which the Supplier shall, and shall procure that any Subcontractor (as applicable) shall, attend.

6. PCI DSS COMPLIANCE AND CERTIFICATION

6.1 Where the Supplier obtains, stores, processes or transmits payment card data, the Supplier shall comply with the PCI DSS.

6.2 The Supplier shall obtain and maintain up-to-date attestation of compliance certificates ("**AoC**") provided by a qualified security assessor accredited by the PCI and up-to-date reports on compliance ("**RoC**") provided by a qualified security assessor or an internal security assessor, in each case accredited by the PCI (each with the content and format as stipulated by the PCI and such reports the "PCI Reports"), during the Call-Off Contract. The Supplier shall provide the respective PCI Reports to the Buyer upon request within 10 Working Days of such request.

6.3 The Supplier shall notify the Buyer of any failure to obtain a PCI Report or a revocation of a PCI Report within 2 Working Days of confirmation of such failure or revocation. The Supplier shall, at its own expense, undertake those actions required

in order to obtain a PCI Report following such failure or revocation within one calendar month of such failure or revocation.

7. SECURITY POLICIES AND STANDARDS

7.1 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.

7.2 Notwithstanding the foregoing, the Buyer's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Variation, any change in the Buyer's Security Requirements resulting from such Variation (if any) shall be agreed by the Parties in accordance with the Variation process detailed at cluse 32 of the Terms and Conditions.

7.3 The Supplier shall, and shall procure that any Subcontractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

8. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

8.1 The Supplier may require a nominated representative of the Supplier to join the Cyber Security Information Sharing Partnership on behalf of the Supplier during the Call-Off Contract, in which case the Supplier's nominated representative shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

8.2 If the Supplier elects a nominated representative to join the Cyber Security Information Sharing Partnership in accordance with Paragraph 9.1 above, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – BUYER SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Physical Security Policy

d) Information Management Policy

e) Email Policy

f) Technical Vulnerability Management Policy

g) Remote Working Policy

h) Social Media Policy

i) Forensic Readiness Policy

j) SMS Text Policy

k) Privileged Users Security Policy

l) User Access Control Policy

m) Security Classification Policy

n) Cryptographic Key Management Policy

o) HMG Personnel Security Controls – May 2018
(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

p) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:
https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) S-002 - PKI & Key Management
d) SS-003 - Software Development
e) SS-005 - Database Management System Security Standard
f) SS-006 - Security Boundaries
g) SS-007 - Use of Cryptography
h) SS-008 - Server Operating System
i) SS-009 - Hypervisor
j) SS-010 - Desktop Operating System
k) SS-011 - Containerisation
l) SS-012 - Protective Monitoring Standard for External Use
m) SS-013 - Firewall Security
n) SS-014 - Security Incident Management
o) SS-015 - Malware Protection
p) SS-016 - Remote Access
q) SS-017 - Mobile Devices
r) SS-018 - Network Security Design
s) SS-019 - Wireless Network
t) SS-022 - Voice & Video Communications
u) SS-023 - Cloud Computing
v) SS-025 - Virtualisation
w) SS-027 - Application Security Testing
x) SS-028 - Microservices Architecture
y) SS-029 - Securely Serving Web Content
z) SS-030 - Oracle Database
aa) SS-031 - Domain Management
bb) SS-033 - Patching