Crown Commercial Service

G-Cloud 9 Call-Off Contract

This Call-Off Contract for the G-Cloud 9 Framework Agreement (RM1557ix) includes:

Part A - Order Form

Digital Marketplace service ID number:	4292 6701 396 2644
Call-Off Contract reference:	ICT12951
Call-Off Contract title:	Crossrail 2 CRM Consultancy Services
Call-Off Contract description:	Microsoft Dynamics CRM support and consultancy services
Start date:	27 July 2018
Expiry date:	26 July 2020 **Optional extension periods:** 1) 27 July 2020 to 26 July 2021 2) 27 July 2021 to 26 July 2022
Call-Off Contract value:	[redacted]
Charging method:	Invoice
Purchase order number:	Purchase Order numbers/lines will be issued in accordance with the SoW process, detailed in Schedule 1

This Order Form is issued under the G-Cloud 9 Framework Agreement (RM1557ix).

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	Transport for London (TfL) 0343 222 1234 Buyer's main address: 55 Broadway, London, SW1H 0BD
To: the Supplier	Codec-dss Ltd Supplier's address: Arnott House (3rd Floor), 12-16 Bridge Street, Belfast, BT1 1LU Company number: NI635500
Together: the 'Parties'	

Principle contact details

For the Buyer:	Title: Mr Name: Robert Marshall (Assistant Commercial Manager) Email: [redacted] Phone: [redacted]
For the Supplier:	Title: Mr Name: John Molloy (UK/NI Commercial Lead) Email: [redacted] Phone: [redacted]

Call-Off Contract term

Start date:	This Call-Off Contract Starts on 10 July 2018 and is valid for 24

	months
Ending (termination):	The notice period needed for Ending the Call-Off Contract is 90 Working Days from the date of written notice for disputed sums or 30 days from the date of written notice for Ending without cause.
Extension period:	This Call-Off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 4 weeks written notice before its expiry. Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.

Buyer contractual details

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

G-Cloud lot:	This Call-Off Contract is for the provision of Services under: Lot 3 - Cloud support
G-Cloud services required:	The Services to be provided by the Supplier under the above Lot are 4292 6701 396 2644 - G-Cloud 9, Cloud Support Services, Dynamics 365 for Education.
Additional services:	Refer to Schedule 1 of this Call-Off contract.
Location:	The Services will be delivered to the Buyer's Location, namely 55 Broadway, London, SW1H 0BD (subject to change). Services will be performed at the Supplier's premises or Buyer's Location as appropriate and as agreed between the Parties from time to time.
Quality standards:	The quality standards required for this Call-Off Contract are ISO 20000
Technical standards:	No additional standards.

Service level agreement:	As per Schedule 1 of this Call-Off Contract.
Onboarding:	The onboarding plan for this Call-Off Contract is as per the agreed transition plan.
Offboarding:	The offboarding plan for this Call-Off Contract is as per the agreed exit plan.
Collaboration agreement:	N/A
Limit on Parties' liability:	The annual total liability of either Party for all Property defaults will not exceed [redacted] [redacted]
Insurance:	The insurance(s) required will be: ● a minimum insurance period of [redacted] following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of [redacted] for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of [redacted] or any higher minimum limit required by Law

Force majeure:	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 30 consecutive days.
Audit:	As per Framework Agreement clauses 7.4 to 7.13
Buyer's responsibilities:	The Buyer shall provide the following to enable the Supplier to undertake the activities required under this Contract: • Access to the Buyer's Location • IT system access • Communication of activities to be undertaken by the assigned Supplier personnel • Coordination with other Buyer teams • User licenses and access to applications • Access to environments for development, test and deployment • Access to repositories for deliverables, including documents, drawings, configuration items, scripts and software code • Infrastructure / network changes • Preparation of training material and conduct of user training • Management and execution of user acceptance testing
Buyer's equipment:	The Buyer shall provide IT system hardware for use at the Buyer's Location.

Supplier's information

Subcontractors or partners:	Not used

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 by bank transfer (Bank Automated Clearance System ("BACS")
Payment profile:	The payment profile for this Call-Off Contract is: 1. For project delivery - milestone payments where services include an agreed Statement of Works identifying such milestones 2. On going support - quarterly in advance 3. Other services - time and materials basis periodically in arrears The Consultant is to provide a 4 weekly update of costs incurred.
Invoice details:	The Supplier will issue electronic invoices in accordance with the Payment profile (above). The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Invoices will be sent to [redacted]
Invoice information required – for example purchase order, project reference:	As a minimum, all invoices must include the following information: - the invoice amount; - the Contract Reference Number; - the Purchase Order number; - the Outline Agreement number; - the Supplier's name and address; - a separate calculation of VAT; and - an adequate description of the Services provided.
Invoice frequency:	Invoice will be sent to the Buyer in accordance with the Payment profile.
Call-Off Contract value:	The total value of this Call-Off Contract is [redacted] over the maximum term of four years
Call-Off Contract charges:	The Charges are based on the standard rate card for Skills of the Information Age (SFIA) published by the Supplier on G-Cloud 9. In consideration of the provision of the G-Cloud Services, the Buyer shall pay the Charges calculated on a time and materials basis (unless otherwise agreed) in accordance with the Supplier's G-Cloud rate

	card, subject to the maximum amount agreed in each Statement of Work and such amount shall not be exceeded unless authorised in writing by the Buyer in advance. The full breakdown of the Charges is shown in Schedule 2 - Call-Off Contract charges. Expenses The Buyer agrees to pay the Supplier [redacted] per full working day when the Supplier's staff are based on-site at the Buyer's Location. No other expenses may be claimed by the Supplier.

Additional buyer terms

Performance of the service and deliverables:	This Call-Off Contract will be managed through a Statement of Works process. The full breakdown of the service is shown in Schedule 1 – Services.
Guarantee:	Not used
Warranties, representations:	As per G-Cloud 9 Framework Agreement clause 4.1.
Supplemental requirements in addition to the Call-Off terms:	The Parties have agreed the additional Call-Off Contract terms: **Intellectual Property Rights** The Supplier will have no rights to use any of the Buyer's names, logos or trademarks without the Buyer's prior written approval. Project Specific IPRs created by the Supplier or any Supplier personnel shall be, and remain, vested in the Buyer. Project Specific IPRs are defined as documents, drawings, configuration artefacts, script, software code and any other work prepared (and identified in the appropriate Statement of Work) for or

	on behalf of the Buyer. **Protection of information** The Supplier will adhere to the Buyer's Data Protection Policy as stated in Schedule 7. **Cyber Security** The Supplier will adhere to the Buyer's most up-to-date cyber security policies, provided in Schedule 8 at the Supplier's request. [redacted]
Alternative clauses:	Not used
Buyer specific amendments to/refinements of the Call-Off Contract terms:	Not used
Public Services Network (PSN):	Not used
Personal Data and Data Subjects:	Refer to Schedule 7 – Processing, Personal Data and Data Subjects

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 and Order Form will supersede those of the Supplier Terms and Conditions.

2. Background to the agreement

(A) The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557ix.

(B) The Buyer provided an Order Form for Services to the Supplier.

Signed:	Supplier	Buyer
Name:	John Molloy	Katerina Kourmpan
Title:	NI Commercial Lead	Senior Commercial Manager
Signature:	[redacted]	[redacted]
Date:		

Schedule 1 - Services

It is acknowledged by the Parties that the volume of the G-Cloud Services utilised by the Buyer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.

The G-Cloud Services to be provided under this Call-Off Agreement will be specified in a Statement of Work. Statement of Works are subject to this Call-Off Agreement and in the event of any conflict, this Call-Off Agreement shall take precedence. Any change to the scope of work shall be agreed between the Parties and documented in revised versions of the affected Statement of Work.

From time to time the Buyer and Supplier may execute a Statement of Work for the G-Cloud Services set out in Buyer Contractual Details section of Part A to this Order form.

The Supplier shall support the Buyer in forming a team to pursue any agreed Statement of Work by providing staff augmentation services. The Supplier and Buyer will agree any changes to the Supplier's personnel provided under this Contract, in advance of the changes being made

Each Statement of Work shall have a unique reference number. Multiple Statements of Work may be used to deliver the G-Cloud Services under this Call-Off Agreement

The Scope of Services may include those listed under section 2.1 of the Supplier's G-Cloud 9 Service Definition document, more specifically the Services must include, but are not be limited to:

- MS Dynamics 365, MS Portals and the Click Dimensions Development, UAT and Production environments;
- Any customisations or configuration changes performed by the Supplier;
- Any add-on products;
- Environment refresh (from Development to UAT and on to Production); and
- A performance health check will be requested.

Functional Support: a second line service for the "how do I?" queries that allow the Supplier to transfer Microsoft (MS) Dynamics 365, MS Portals and Click Dimensions knowledge to the Buyer.

Technical Incident Support: a second line service for Buyer nominated representatives to report technical issues defined as Incidents, to the Supplier to manage through to resolution.

Change Advisory Support: representation at the Buyer's Change Advisory Board to ensure that Buyer led changes to the MS Dynamics, Portals and Click Dimensions systems do not negatively impact the existing solution design.

Communication: The provision of a telephone support number and support portal that can be used to contact the Supplier. The Buyer will provide no more than five nominated first line support contacts.

Supplier's Key Personnel

Name & Position	**Contact Details**	**Area of Responsibility**
John Molloy Ni Commercial Lead	[redacted]	Commercial and Account Management, overall responsibility for the contract and relationship.
Brian Illand Microsoft Practice Lead	[redacted]	Overall Solution Architect and Practice Team lead/manager
Gee Lau Senior CRM Consultant	[redacted]	Function Design Lead, key engagement around understanding requirements at a functional level.
Pamela Ross Business Consulting Manager	[redacted]	Program and project management within the Codec team.

Service Level Agreement for ongoing support:

Method	Initial Response	Details
Phone (normal working hours)	Immediate – the phones are manned by our Service Desk engineers.	
Email	Within 30 minutes – emails to our. Service Desk are managed by one of our call schedulers who will respond with confirmation of receipt of email, call log number and assigned engineer.	[redacted]
Web Portal	Within 30 minutes. Issues logged to our Web Portal are notified to our call schedulers who will respond with confirmation of receipt of issue logged, a call log number will be assigned and the web portal updated with relevant information.	[redacted]

Schedule 2 - Call-Off Contract charges

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

Skills For the Information Age (SFIA) Definitions & Rate Card

Supplier's Standard Rate Card

	Strategy & architecture	Business change	Solution development & implementation	Service management	Procurement & management support	Client interface
1. Follow	£500.00	£500.00	£500.00	£500.00	£500.00	£500.00
2. Assist	£570.00	£570.00	£570.00	£570.00	£570.00	£570.00
3. Apply	£680.00	£680.00	£680.00	£680.00	£680.00	£680.00
4. Enable	£730.00	£730.00	£730.00	£730.00	£730.00	£730.00
5. Ensure/Advise	£750.00	£750.00	£750.00	£750.00	£750.00	£750.00
6. Initiate/Influence	£750.00	£750.00	£750.00	£750.00	£750.00	£750.00
7. Set Strategy/Inspire	£830.00	£830.00	£830.00	£830.00	£830.00	£830.00

Supplier discount structure

Discounts applicable:

Discount for 51 - 99 days 6%

Discount for 100+ days 8.5%

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, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

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

2. Incorporation of terms

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

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)

- 8.4 (Relationship)
- 8.7 to 8.9 (Entire agreement)
- 8.10 (Law and jurisdiction)
- 8.11 to 8.12 (Legislative change)
- 8.13 to 8.17 (Bribery and corruption)
- 8.18 to 8.27 (Freedom of Information Act)
- 8.28 to 8.29 (Promoting tax compliance)
- 8.30 to 8.31 (Official Secrets Act)
- 8.32 to 8.35 (Transfer and subcontracting)
- 8.38 to 8.41 (Complaints handling and resolution)
- 8.49 to 8.51 (Publicity and branding)
- 8.42 to 8.48 (Conflicts of interest and ethical walls)
- 8.52 to 8.54 (Equality and diversity)
- 8.66 to 8.67 (Severability)
- 8.68 to 8.82 (Managing disputes)
- 8.83 to 8.91 (Confidentiality)
- 8.92 to 8.93 (Waiver and cumulative remedies)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretations
- 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:

- a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- a reference to 'CCS' will be a reference to 'the Buyer'
- 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 Framework Agreement incorporated clauses will be referred to as 'incorporated Framework clause XX', where 'XX' is the Framework Agreement clause number.

2.4 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:

- be appropriately experienced, qualified and trained to supply the Services
- apply all due skill, care and diligence in faithfully performing those duties
- obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
- respond to any enquiries about the Services as soon as reasonably possible
- 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 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:

- have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
- are confident that they can fulfil their obligations according to the Call-Off Contract terms
- have raised all due diligence questions before signing the Call-Off Contract
- 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 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:

- 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 [redacted]

- the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit
- all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of [redacted] for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
- all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of [redacted] for each individual claim during the Call-Off Contract, [redacted]

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:

- a broker's verification of insurance
- receipts for the insurance premium
- 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:

- take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- promptly notify the insurers in writing of any relevant material fact under any insurances
- 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:

- premiums, which it will pay promptly
- 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 8.83 to 8.91. 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:

- rights granted to the Buyer under this Call-Off Contract
- Supplier's performance of the Services
- 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:

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

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

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

- providing the Buyer with full details of the complaint or request
- complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
- providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
- 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

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

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

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

13.3 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 policy and all Buyer requirements in the Order Form.

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

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

- the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
- 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, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- the security requirements of cloud services using the NCSC Cloud Security

Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

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

13.7 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.

13.8 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.

13.9 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 available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

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

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

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN

Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

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

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use 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:

- 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

- 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 CCS of any breach of security of CCS'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 CCS and Buyer 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, available at 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:

- an executed Guarantee in the form at Schedule 5
- 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 the notice to the Supplier 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:

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

- a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- any fraud

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

- 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
- an Insolvency Event of the other Party happens
- 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:

- any rights, remedies or obligations accrued before its Ending or expiration
- the right of either Party to recover any amount outstanding at the time of Ending or expiry
- 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); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)
- 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:

- return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- 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
- 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
- work with the Buyer on any ongoing work
- 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	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an 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:

- 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
- there will be no adverse impact on service continuity
- there is no vendor lock-in to the Supplier's Service at exit
- 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:

- 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
- 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
- the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- the testing and assurance strategy for exported Buyer Data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- 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:

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

- Property: for all defaults 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
- Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
- Other defaults: for all other defaults, 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:

- comply with any security requirements at the premises and not do anything to weaken the security of the premises
- comply with Buyer requirements for the conduct of personnel
- comply with any health and safety measures implemented by the Buyer
- 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:

- the activities they perform
- age
- start date
- place of work
- notice period
- redundancy payment entitlement
- salary, benefits and pension entitlements
- employment status
- identity of employer
- working arrangements
- outstanding liabilities
- sickness absence
- copies of all relevant employment contracts and related documents
- 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:

- its failure to comply with the provisions of this clause
- 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 in the form set out in Schedule 3.

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

- work proactively and in good faith with each of the Buyer's contractors
- 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 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the

Supplier will promptly notify the Buyer of any additional processing if permitted by Law).

33.2 The Supplier will provide all reasonable assistance to the Buyer to prepare any Data Protection Impact Assessment before commencing any processing (including provision of detailed information and assessments in relation to processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer's instructions infringe the Data Protection Legislation.

33.3 The Supplier must have in place Protective Measures, which have been reviewed and approved by the Buyer as appropriate, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Personnel only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier Personnel with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier's obligations under this Clause;

ii) are subject to appropriate confidentiality undertakings with the Supplier or relevant Subprocessor

iii) are informed of the confidential nature of the Personal Data and don't publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract

iv) are given training in the use, protection and handling of Personal Data.

33.5 The Supplier will not transfer Personal Data outside of the European Economic Area unless the prior written consent of the Buyer has been obtained and

i) the Buyer or the Supplier has provided appropriate safeguards in relation to the

transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Buyer;

ii) the Data Subject has enforceable rights and effective legal remedies;

iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Buyer in meeting its obligations); and

iv) the Supplier complies with any reasonable instructions notified to it in advance by the Buyer with respect to the processing of the Personal Data.

33.6 The Supplier will delete or return Buyer's Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

33.7 The Supplier will notify the Buyer immediately if it receives any communication from a third party relating to the Parties' obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party's obligations under the Data Protection Legislation in accordance with any timescales reasonably required by the Buyer.

33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

i) the Buyer determines that the processing is not occasional;

ii) the Buyer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

iii) the Buyer determines that the processing is likely to result in a risk to the rights

and freedoms of Data Subjects.

33.9 Before allowing any Subprocessor to process any Personal Data related to this Call-Off Contract, the Supplier must obtain the prior written consent of the Buyer, and shall remain fully liable for the acts and omissions of any Subprocessor.

33.10 The Buyer may amend this Call-Off Contract on not less than 30 Working Days' notice to the Supplier to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 5 - Guarantee

The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents

Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

	Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement 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 Data Protection Legislation.
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	Any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Call-Off Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Call-Off Contract, including any Personal Data Breach.
Data Protection Impact Assessment	An assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
Data Protection Legislation	Data Protection Legislation means: i) all applicable Law about the processing of personal data and privacy; and ii) ii) The Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice)

	(Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 including if applicable legally binding guidance and codes of practice issued by the Information Commissioner; and iii) iii) to the extent that it relates to processing of personal data and privacy, any Laws that come into force which amend, supersede or replace existing Laws including the GDPR, the LED and any applicable national implementing Laws as amended from time to time including the DPA 2018 [subject to Royal Assent].
Data Subject	Takes the meaning given in the Data Protection Legislation.
Default	Default is any: ● breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) ● other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
Deliverable	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for

	Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
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 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: http://tools.hmrc.gov.uk/esi
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 RM1557ix 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	The 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.
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.
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.
Key Personnel	The Supplier's key personnel named in Schedule 1
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 applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.
LED	Law Enforcement Direction (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	[redacted]
Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.

Ordered G-Cloud Services	G-Cloud Services which are the subject of an Order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the Data Protection Legislation.
Personal Data Breach	Takes the meaning given in the Data Protection Legislation.
Processing	This has the meaning given to it under the General Data Protection Regulation (GDPR) 2016/679 as amended but, for the purposes of this Call-Off Contract, it will include both manual and automatic processing. 'Process' and 'processed' will be interpreted accordingly.
Processor	Takes the meaning given in the Data Protection Legislation.
Prohibited Act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud

	○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the Government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory Body or Bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant Person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the Employment Regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement Supplier	Any third party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
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 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 - Processing, Personal Data and Data Subjects

A1 Privacy and Data Protection

For the purposes of this Clause A1, unless the context indicates otherwise, the following expressions shall have the following meanings:

"Buyer Personal Data"	Personal Data and/or Sensitive Personal Data Processed by the Supplier or any sub-contractor on behalf of the Buyer, pursuant to or in connection with this Contract;
"Data Controller"	has the meaning given to it in Data Protection Legislation;
"Data Processor"	has the meaning given to it in Data Protection Legislation;
"Data Protection Impact Assessment"	a process used to identify and mitigate the privacy and data protection risks associated with an activity involving the Processing of Personal Data;
"Data Protection Legislation"	means: (a) any legislation in force from time to time in the United Kingdom which implements the European Community's Directive 95/46/EC and Directive 2002/58/EC, including but not limited to the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003; (b) from 25 May 2018 only, the Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data (the "General Data Protection Regulation");

	(c) any other legislation in force from time to time in the United Kingdom relating to privacy and/or the Processing of Personal Data; and (d) any statutory codes of practice issued by the Information Commissioner in relation to such legislation;
"Data Subject"	has the meaning given to it in Data Protection Legislation;
"Personal Data"	has the meaning given to it in Data Protection Legislation;
"Processing"	has the meaning given to it in Data Protection Legislation and "Process" and "Processed" will be construed accordingly;
"Restricted Countries"	any country outside the European Economic Area;
"Sensitive Personal Data"	sensitive or special categories of Personal Data (as defined in Data Protection Legislation) which is Processed pursuant to or in connection with this Contract; and
"Subject Access Request"	a request made by a Data Subject to access his or her own Personal Data in accordance with rights granted in Data Protection Legislation.

A1.1 With respect to the Parties' rights and obligations under the Contract, the Parties acknowledge that the Buyer is a Data Controller solely responsible for determining the purposes and manner in which Buyer Personal Data is to be Processed, and that the Supplier is a Data Processor.

A1.2 Details of the Buyer Personal Data to be Processed by the Supplier and the purposes of such Processing are as follows:

A1.2.1 The Buyer Personal Data to be Processed by the Supplier (if any) concerns the following categories of Data Subject:

Crossrail 2 Staff

Private Individuals

Politicians (MPs, councillors, assembly members)

All those who have signed up to receive Crossrail2 updates

All those who have responded to a previous consultation

All those who have called the Crossrail 2 helpline

Local stakeholders – MPs, councillors, businesses, individual residents, property addresses/names

A1.2.2 The Buyer Personal Data to be Processed includes the following types of Personal Data and/or Sensitive Personal Data:

Names, addresses, telephone numbers, email addresses and other contact details

Consultation responses

Electronic records of emails, phone calls, minutes

Emails between Crossrail 2 staff and members of the public/MPs, councillors, internal briefings

Names and address lists of all those we have written to in the past – eg, MPs, businesses, councillors, property owners/occupiers of directly affected properties, or who Crossrail2 proposed to write to since the postponed consultations

Lists of local stakeholders – MPs, councillors, businesses, individual residents, property addresses/names

A1.2.3 The Buyer Personal Data is to be Processed for the following purpose(s):

Support arguments for/against design aspects such as, but not limited to, route, stations, and regeneration

Produce briefing documents for senior staff, politicians and stakeholders

To provide data to our contractors and suppliers to aid decisions on design, demand, footfall

To satisfy statutory obligations on consultations

To provide data for the Crossrail2 website and other publications

A1.2.4 The Buyer Personal Data is to be Processed in the following Restricted Countries:

None outside the EU

A1.3 The Supplier shall:

A1.3.1 process the Buyer Personal Data only in accordance with instructions from the Buyer to perform its obligations under the Contract;

A1.3.2 use its reasonable endeavours to assist the Buyer in complying with any obligations under Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Buyer to breach any of its obligations under Data Protection Legislation to the extent the Supplier is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations;

A1.3.3 notify the Buyer without undue delay if it determines or is notified that an instruction to Process Personal Data issued to it by the Buyer is incompatible with any obligations under Data Protection Legislation to the extent the Supplier is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations;

A1.3.4 maintain, and make available to the Buyer on its request, documentation which describes the Processing operations for which it is responsible under this Contract including:

A1.3.4.1 the purposes for which Buyer Personal Data is Processed;

A1.3.4.2 the types of Personal Data and categories of Data Subject involved;

A1.3.4.3 the source(s) of the Personal Data;

A1.3.4.4 any recipients of the Personal Data;

A1.3.4.5 the location(s) of any overseas Processing of Buyer Personal Data;

A1.3.4.6 retention periods for different types of Buyer Personal Data; and

A1.3.4.7 where possible a general description of the security measures in place to protect Buyer Personal Data.

A1.3.5 where requested to do so by the Buyer, or where Processing Buyer Personal Data presents a specific risk to privacy, carry out a Data Protection Impact Assessment in accordance with guidance issued from time to time by the Information Commissioner (and any relevant requirements detailed in Data Protection Legislation) and make the results of such an assessment available to the Buyer;

A1.3.6 without prejudice to any cyber security and/or payment card industry data security standard obligations in this Contract, take appropriate technical and organisational security measures that are satisfactory to the Buyer from time to time, against unauthorised or unlawful Processing of Buyer Personal Data and against accidental loss, destruction of, or damage to such Buyer Personal Data;

A1.3.7 without prejudice to any cyber security and/or payment card industry data security standard obligations in this Contract, provide the Buyer with such

information as the Buyer may from time to time require to satisfy itself of compliance by the Supplier (and/or any authorised sub-contractor) with Clauses A1.3.6 and A1.3.8, including, protocols, procedures, guidance, training and manuals. For the avoidance of doubt, this shall include a full report recording the results of any privacy or security audit carried out at the request of the Supplier itself or the Buyer;

A1.3.8 notify the Buyer without undue delay and in any event within 24 hours by written notice with all relevant details reasonably available of any actual or suspected breach of this Clause A1, including the unauthorised or unlawful Processing of Buyer Personal Data, or its accidental loss, destruction or damage;

A1.3.9 having notified the Buyer of a breach in accordance with Clause A1.3.8, keep the Buyer properly and regularly informed in writing until the breach has been resolved to the satisfaction of the Buyer;

A1.3.10 fully cooperate as the Buyer requires with any investigation or audit in relation to Buyer Personal Data and/or its Processing including allowing access to premises, computers and other information systems, records, documents and agreements as may be reasonably necessary (whether in relation to Processing pursuant to the Contract, in relation to compliance with Data Protection Legislation or in relation to any actual or suspected breach), whether by the Buyer (or any agent acting on its behalf), any relevant regulatory body, including the Information Commissioner, the police and any other statutory law enforcement agency, and shall do so both during the Contract and after its termination or expiry (for so long as the Party concerned retains and/or Processes Buyer Personal Data);

A1.3.11 notify the Buyer within two (2) Business Days if it, or any sub-contractor, receives:

A1.3.11.1 from a Data Subject (or third party on their behalf):

A1.3.11.1.1 a Subject Access Request (or purported Subject Access Request);

A1.3.11.1.2 a request to rectify, block or erase any Buyer Personal Data; or

A1.3.11.1.3 any other request, complaint or communication relating to the Buyer's obligations under Data Protection Legislation.

A1.3.11.2 any communication from the Information Commissioner or any other regulatory authority in connection with Buyer Personal Data; or

A1.3.11.3 a request from any third party for disclosure of Buyer Personal Data where compliance with such request is required or purported to be required by law;

A1.3.12 provide the Buyer with full cooperation and assistance (within the timescales reasonably required by the Buyer) in relation to any complaint, communication or request made as referred to in Clause A1.3.11, including by promptly providing:

A1.3.12.1 the Buyer with full details and copies of the complaint, communication or request;

A1.3.12.2 where applicable, such assistance as is reasonably requested by the Buyer to enable it to comply with the Subject Access Request within the relevant timescales set out in Data Protection Legislation; and

A1.3.12.3 where applicable, such assistance as is reasonably required by the Buyer to enable it to comply with a request from a Data Subject to rectify, block or erase any Buyer Personal Data.

A1.3.13 when notified in writing by the Buyer, supply a copy of, or information about, any Buyer Personal Data. The Supplier shall supply such information

or data to the Buyer within such time and in such form as specified in the request (such time to be reasonable) or if no period of time is specified in the request, then within two (2) Business Days from the date of the request;

A1.3.14 when notified in writing by the Buyer, comply with any agreement between the Buyer and any Data Subject in relation to any Processing which causes or is likely to cause substantial and unwarranted damage or distress to such Data Subject, or any court order requiring the rectification, blocking, erasure or destruction of any Buyer Personal Data; and

A1.3.15 if required to do so by Data Protection Legislation, appoint a designated Data Protection Officer.

A1.4 The Supplier shall not share Buyer Personal Data with any sub-contractor without prior written consent from the Buyer and only where there is a written contract in place between the Supplier and the sub-contractor which requires the sub-contractor to:

A1.4.1 only Process Buyer Personal Data in accordance with the Buyer's instructions to the Supplier; and

A1.4.2 comply with the same obligations which the Supplier is required to comply with under this Clause A1 (and in particular Clauses 12.1, 16.1, 16.2, 18.1, 20.2, 22 and 23).

A1.5 The Supplier shall, and shall procure that any sub-contractor shall:

A1.5.1 only Process Buyer Personal Data in accordance with the Buyer's instructions to the Supplier and as reasonably necessary to perform the Contract in accordance with its terms;

A1.5.2 not Process Buyer Personal Data for any other purposes (in whole or part) and specifically, but without limitation, reproduce or refer to it in training materials, training courses, commercial discussions and negotiations with third parties or in relation to proposals or tenders with the Buyer;

A1.5.3 not Process Buyer Personal Data in such a way as to:

A1.5.3.1 place the Buyer in breach of Data Protection Legislation;

A1.5.3.2 expose the Buyer to the risk of actual or potential liability to the Information Commissioner or Data Subjects;

A1.5.3.3 expose the Buyer to reputational damage including adverse publicity;

A1.5.4 not allow Supplier's Personnel to access Buyer Personal Data unless such access is necessary in connection with the provision of the Services;

A1.5.5 take all reasonable steps to ensure the reliability and integrity of all Supplier's Personnel who can access Buyer Personal Data;

A1.5.6 ensure that all Supplier's Personnel who can access Buyer Personal Data:

A1.5.6.1 are informed of its confidential nature;

A1.5.6.2 are made subject to an explicit duty of confidence;

A1.5.6.3 understand and comply with any relevant obligations created by either this Contract or Data Protection Legislation; and

A1.5.6.4 receive adequate training in relation to the use, care, protection and handling of Personal Data on an annual basis.

A1.5.7 not disclose or transfer Buyer Personal Data to any third party without the Supplier having obtained the prior written consent of the Buyer (save where such disclosure or transfer is specifically authorised under this Contract);

A1.5.8 without prejudice to Clause A1.3.6, wherever the Supplier uses any mobile or portable device for the transmission or storage of Buyer Personal Data, ensure that each such device encrypts Buyer Personal Data; and

A1.5.9 comply during the course of the Contract with any written retention and/or deletion policy or schedule provided by the Buyer to the Supplier from time to time.

A1.6 The Supplier shall not, and shall procure that any sub-contractor shall not, Process or otherwise transfer any Buyer Personal Data in or to any Restricted Countries without prior written consent from the Buyer (which consent may be subject to additional conditions imposed by the Buyer)**.**

A1.7 If, after the Service Commencement Date, the Supplier or any sub-contractor wishes to Process and/or transfer any Buyer Personal Data in or to any Restricted Countries, the following provisions shall apply:

A1.7.1 the Supplier shall submit a written request to the Buyer setting out details of the following:

A1.7.1.1 the Buyer Personal Data which will be transferred to and/or Processed in any Restricted Countries;

A1.7.1.2 the Restricted Countries which the Buyer Personal Data will be transferred to and/or Processed in;

A1.7.1.3 any sub-contractors or other third parties who will be Processing and/or receiving Buyer Personal Data in Restricted Countries;

A1.7.1.4 how the Supplier shall ensure an adequate level of protection and adequate safeguards in respect of the Buyer Personal Data that will be Processed in and/or transferred to Restricted Countries so as to ensure the Buyer's compliance with Data Protection Legislation;

A1.7.2 in preparing and evaluating such a request, the Parties shall refer to and comply with applicable policies, procedures, guidance and codes of practice produced by the Parties and/or the Information Commissioner in connection with the Processing of Personal Data in (and/or transfer of Personal Data to) any Restricted Countries;

A1.7.3 the Supplier shall comply with any instructions and shall carry out such actions as the Buyer may notify in writing when providing its consent to such Processing or transfers, including:

A1.7.3.1 incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) into this Contract or a separate data processing agreement between the Parties; and

A1.7.3.2 procuring that any sub-contractor or other third party who will be Processing and/or receiving or accessing the Buyer Personal Data in any Restricted Countries enters into a data processing agreement with the Supplier on terms which are equivalent to those agreed between the Buyer and the Supplier in connection with the Processing of Buyer Personal Data in (and/or transfer of Buyer Personal Data to) any Restricted Countries, and which may include the incorporation of the clauses referred to in A1.7.3.1.

A1.8 The Supplier and any sub-contractor (if any), acknowledge:

A1.8.1 the importance to Data Subjects and the Buyer of safeguarding Buyer Personal Data and Processing it only in accordance with the Buyer's instructions and the Contract;

A1.8.2 the loss and damage the Buyer is likely to suffer in the event of a breach of the Contract or negligence in relation to Buyer Personal Data;

A1.8.3 any breach of any obligation in relation to Buyer Personal Data and/or negligence in relation to performance or non performance of such obligation shall be deemed a material breach of Contract;

A1.8.4 notwithstanding Clause 26.1.1, if the Supplier has committed a material breach under Clause A1.8.3 on two or more separate occasions, the Buyer may at its option:

A1.8.4.1 exercise its step in rights pursuant to Clause A16;

A1.8.4.1 withdraw authorisation for Processing by a specific sub-contractor by immediate written notice; or

A1.8.4.2 terminate the Contract in whole or part with immediate written notice to the Supplier.

A1.9 Compliance by the Supplier with this Clause A1 shall be without additional charge to the Buyer.

A1.10 Following termination or expiry of this Contract, howsoever arising, the Supplier:

A1.12.1 may Process the Buyer Personal Data only for so long and to the extent as is necessary to properly comply with its non-contractual obligations arising under law (and will then comply with Clause A1.10.2);

A1.12.2 subject to Clause A1.10.1, shall;

A1.10.2.1 on written instructions from the Buyer either securely destroy or securely and promptly return to the Buyer or a recipient nominated by the Buyer (in such usable format as and to the extent the Buyer may reasonably require) the Buyer Personal Data; or

A.10.2.2 in the absence of instructions from the Buyer after 12 months from the expiry or termination of the Contract securely destroy the Buyer Personal Data.

A1.11 Buyer Personal Data may not be Processed following termination or expiry of the Contract save as permitted by Clause A1.10.

A1.12 For the avoidance of doubt, and without prejudice to Clause A1.10, the obligations in this Clause A1 shall apply following termination or expiry of the Contract to the extent the Party concerned retains or Processes Buyer Personal Data.

A1.13 The indemnity in Clause 18 shall apply to any breach of Clause A1 and shall survive termination or expiry of the Contract.

A1.14 The Parties' liability in respect of any breach of Clause 22.1 and this Clause A1 insofar as they relate to fines, court awards, settlements and legal costs shall be unlimited.

Schedule 8 – Cyber Security Management

For the purposes of this Call-Off Contract being provided by the Supplier, the definition of the Services includes the devices and networks used by the Supplier to access the Dynamics Platform to deliver the required configuration and support. Also included will be the code developed by the Supplier for implementation in the environment.

The Microsoft Dynamics 365 Environment is out of scope for the purposes of this Schedule as this platform is provided to the Supplier on behalf of Buyer by Microsoft. The Supplier has no responsibility for the availability of the overall platform.

The Security Manager will be John Molloy; this is a point of contact for any security breaches.

The security management plan will be formed on the basis of the accreditations in place including Cyber Security Essentials.

1. DEFINITIONS

"Cloud"	A type of internet-based computing service where organisation can have aspects of their IT infrastructure managed by external providers, normally as a Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) basis
"Cyber Essentials Scheme"	is a UK government scheme encouraging organisations to adopt good practice in information security, focussing mainly on technical controls rather than governance, risk, and policy
"Cyber Security Policy / Policies"	The high level Cyber Security requirements for all IT and Operational technology and data owned by TfL or operated and supported by third parties for on behalf of TfL.

"Cyber Security Standard(s)"	The technical detail behind the implementation of the high level cyber security requirements as set out in the Cyber Security Policies.
"Data"	means data created, generated or collected, during the performance of the Services (or any part thereof), including Personal Data and data supplied to TfL and members of the TfL Group in connection with the Services or this Agreement;
"Good Industry Practice"	means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in the same type of undertaking under the same or similar circumstances.
HMG Information Security Assurance Standards	the meaning and definition as well as relevant policy documents and standards can be found at https://www.gov.uk/government/collections/government-security or any updated link;
"Information Asset Register"	means a register of all information assets relating to the services connected to this Agreement as detailed in paragraph 3.2(c)
"Information Security Management System" or "ISMS"	a framework of governance models, policies and procedures, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security in accordance with the requirements of Paragraph 15
ISO/IEC 27001	is an information security standard specification for an information security management system (ISMS), with an emphasis on measuring and evaluating how

	well an organisation's ISMS is performing.
"IT Services"	means the IT services that support the delivery of the Services;
"Malicious Software"	means any software that brings harm to a computer system. Commonly known as malware can be in the form of worms, viruses, trojans, spyware, and adware which steal protected data, delete documents or add software not approved by a user.
"Operational Technology"	means any hardware or software which monitors and/or operates a physical process.
"Outline Security Management Plan"	means the security plan provided by the Supplier as part of their tender submission
"Removable Media"	any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives
"Security Incident"	a potential or actual event or attempted breach of security affecting the confidentiality, integrity or availability of the Services, IT Services or Networks which process or hold Data
"Security Management Plan"	means the Supplier's security plan developed and revised pursuant to Paragraph 14
"Security Policy"	means any TfL security policies as amended by TfL from time to time;

"Security Risk"	meaning all Risks associated with the security of the Services which may have a negative impact upon the agreed security posture, including information security and any risks identified pursuant to the Security Management Schedule.
"Security Risk Register"	means a register of Security Risks produced and maintained as detailed in paragraph 3.2(b)
"Service Assets"	means all assets and rights including all physical assets, Software, IPR, as well as spares and components whether in storage, repair or on sites, used by the Supplier to provide the Services in accordance with this Agreement;
"Supplier Personnel"	means all employees, agents, consultants and contractors of the Supplier or of any Sub-Contractor
"Supplier Premises"	means any land or building where the Supplier carries out any part of this contract
"TfL Information Security Controls Framework"	means a hierarchy of IT security documents consisting of the high level Information Management Security Policy and ten security principles (Information Security Controls Framework) available upon request.
"TfL Network(s)"	means the network infrastructure and services owned or used by TfL to support the delivery of the IT Services.
"TfL Personnel "	means all employees, agents, consultants and contractors of TfL
"TfL	as defined in the TfL Information Security

Restricted"	Classification Standard (listed in Annex 5)
"TfL Sites"	means all TfL premises where the services are delivered

2. SCOPE AND PURPOSE

2.1 The purpose of this Schedule is to:

(a) set out the principles of protective security to be applied by the Supplier in its delivery of the Services;

(b) set out the Supplier's wider security obligations relating to the Services;

(c) set out the Supplier's requirements to test and audit the Services including any Information Security Management System, to ensure compliance with the security requirements set out in this Agreement;

(d) set out the Supplier's obligations in the event of a Security Incident;

(e) set out the principles for the Supplier's development, implementation, operation, maintenance and continual improvement of the Security Management Plan;

(f) set out the principles for the Supplier's development, implementation, operation, maintenance and continual improvement of the Information Security Management System;

(g) set out any Supplier obligation for certification against the Services such as, ISO/IEC 27001, the Cyber Essentials Scheme or HMG Information Security Assurance Standards;

(h) set out any Supplier requirements to deliver the Services or Service Assets in accordance with the CESG Commercial Product Assurance (CPA) Scheme; and

(i) set out the requirements on the Supplier when delivering the Service(s), which are aligned with the 10 Steps to Cyber security set out by the Government (see Annex 5).

(j) the Supplier's obligation to comply with the Operations Technology Cyber Security Standards (see Annex 5).

3. SECURITY PRINCIPLES

3.1 The Supplier acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its provision of the Services and TfL's ability to retain public confidence. The Supplier shall at all times comply with the security principles set out in Paragraph 3 in the delivery of the Services.

3.2 In recognition of the importance that TfL places on security, data protection and confidentiality, the Supplier shall ensure that a director or relevant individual, as agreed by TfL, is made aware of the risks set out in the Security Management Plan and is assigned overall responsibility for ensuring that:

(a) appropriate members of Supplier Personnel and the Supplier's management team take responsibility for managing the different levels of security risk and promoting a risk management culture;

(b) a Security Risk Register is produced and maintained and that all Security Risks are documented in an appropriate manner and is included in any contract risk register if one is in place. This Security Risk Register must be available for audit when reasonably required by TfL as set out in Clause 7 of this Schedule

(c) an Information Asset Register is produced and maintained and that all assets are documented in an appropriate manner in the Information Asset Register and shall identify the criticality of the relevant Service Assets in the delivery of the Services. This register must be available for audit when reasonably required by TfL as stated in Paragraph 7 of this Schedule and when a Security Incident occurs.

(d) supporting policies are implemented (where relevant) and communicated with Supplier Personnel.

3.3 The Supplier shall, and procure that its Sub-contractors shall, at all times ensure that:

(a) security threats to the Services are minimised and mitigated;

(b) the Services shall fully comply at all times with:

(i) any security requirements set out in Annex 3;

(ii) the agreed Outline Risk Management Processes and approach set out in Annex 2; and

(iii) Good Industry Practice.

3.4 The Supplier must notify TfL of any instances where software, applications, services or processes are hosted or run from the cloud that are not part of the Agreement, and that host, process or connect with any of TfL Operational or IT technology, Data and Networks or handle TfL Data. The Supplier is responsible for ensuring that any such cloud services comply with this Cyber Security Management Schedule.

4. ACCESS CONTROLS AND SECURE CONFIGURATION OF SYSTEMS

4.1 The Supplier shall comply with all obligations relating to the patching and configuration management of Service Assets as set out in Annex 4 in addition to any specific obligations set out in Annex 4, the Supplier shall ensure that:

(a) security patches are applied to Service Assets as soon as possible in line with vendor recommendations in accordance with overall risk management;

(b) account management and configuration control processes are implemented to ensure that access to Service Assets by Supplier Personnel is limited to the extent required for them to fulfil their roles in supporting the delivery of the Services.

(c) when Supplier Personnel change roles or no longer support the delivery of the Services access rights are revoked or reviewed;

(d) any system administration functionality is strictly controlled and restricted to those Supplier Personnel who need to have access to such functionality and that the ability of Supplier Personnel to change the configuration of the Services is appropriately limited and fully auditable;

(e) Supplier Personnel are informed of what constitutes acceptable access of Operational or IT technology, Data and Networks and the consequences of non-compliance;

(f) any preconfigured passwords delivered with any Service Assets are changed prior to their implementation for use in the Services;

(g) the Services have appropriate devices, tools or applications in place to filter traffic or separate connections, such as industry standard firewalls and Malicious Software protection, to all public or private networks which are not controlled by or on behalf of TfL.

(h) all wireless functionality is secure; and

(i) software upgrades and patching must be managed appropriately and access to any software shall be granted using the principle of least privilege.

5. SUPPLIER PERSONNEL

5.1 The Supplier shall, appoint a member of Supplier Personnel to be the security manager who shall be responsible for the development, monitoring, enforcement, maintenance and enhancement of all security measures set out in this Agreement (the "**Security Manager**"). The Security Manager shall be a member of the Key Personnel.

5.2 The Supplier shall ensure that all Supplier Personnel are security screened or vetted appropriate to the Data and shall provide TfL within five (5) working days of the Start Date, and every twelve (12) months thereafter, written confirmation that this obligation has been complied with.

5.3 The Supplier shall immediately notify TfL if it becomes aware of any security clearance issues in relation to the Supplier Personnel and the Supplier shall undertake any action requested by TfL in relation to mitigating the impact of any such security clearance issues.

5.4 The Supplier shall not remove or replace the Security Manager (including when carrying out Exit Management) unless:

(a) requested to do so by TfL;

(b) the Security Manager concerned resigns, retires or dies or is on maternity, paternity, adoption or long-term sick leave;

(c) the Security Manager's employment or contractual arrangement with the Supplier or a Sub-contractor is terminated for material breach of contract by that person; or

(d) the Supplier obtains TfL's prior written consent (such consent not to be unreasonably withheld or delayed) and the role is not left vacant.

5.5 The Supplier shall:

(a) notify TfL promptly of the absence of the Security Manager (other than for short-term sickness or holidays of three (3) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for Security Manager);

(b) ensure that Security Manager role is not vacant for any longer than fifteen (15) Working Days;

(c) give as much notice to TfL as is reasonably practicable (and in any event twenty (20) Working Days' notice) of any intention to remove or replace Security Manager except in the cases of death, unexpected ill health or a material breach by the Security Manager of his or her employment contract;

(d) ensure that all arrangements for planned changes in the Security Manager provide adequate periods during which incoming and outgoing Security Manager work together to transfer responsibilities and ensure that such change does not have an adverse impact on the performance of the Services; and

(e) ensure that any replacement for the Security Manager

(i) is only employed or engaged with TfL's prior written consent (such consent not to be unreasonably withheld or delayed)

(ii) has a level of qualifications and experience appropriate for a Security Manager; and

(iii) is fully competent to carry out the tasks of a Security Manager whom he or she has replaced.

6. TRAINING

6.1 The Supplier shall ensure that all Supplier Personnel have undergone suitable security awareness training prior to their deployment and such security awareness training shall cover, as a minimum; account usage, malicious software, home and mobile working, use of removable media, audit and inspection and Security Incident reporting and data handling. The Supplier shall implement an up-to-date on-going programme of security awareness training for Supplier Personnel throughout the Term.

6.2 The Supplier shall provide additional training to its Supplier Personnel, which may be required following a Security Incident, the application of a patch or update, or any relevant Operational Change or Variation.

6.3 The Supplier shall ensure that all Supplier Personnel are familiar with their responsibilities under applicable law and policies including, as a minimum, the Data Protection Legislation, the Security Policies set out in Paragraph 1 of this Schedule and policies in relation to the handling of protectively marked materials both during their employment and following the termination of or change to the terms of their employment.

7. TESTING & AUDIT

7.1 The Supplier shall conduct regular automated vulnerability scans of the Services, as agreed in the Risk Management Process and ensure that any identified vulnerabilities are appropriately mitigated or patched in line with the TfL Security Patching standard (Annex 5), taking into consideration the risk posed to TfL and the Services.

7.2 The Supplier shall conduct security tests, including ethical hacking and penetration tests, to assure compliance with the Security Incident Management Process, the security provisions in this Agreement, the Security Management Plan. The Supplier shall conduct security testing in accordance with the Security Management Plan. The Supplier shall conduct such security tests, as a minimum, every twelve (12) months from the Service Commencement Date and shall include security penetration testing of the Services and the associated technical infrastructure. Wherever the Services are accessible from the internet or other such public network, the Supplier shall carry out security penetration tests from the internet or the public network.

7.3 The Supplier shall, within one (1) week completion of the security tests carried out in accordance with Paragraph 7.2, provide a report to TfL setting out:

(a) the outcome of such security tests including all identified vulnerabilities;

(b) the Supplier's plans to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement including the TfL Change Management Process and the Variation Procedure.

7.4 The Supplier shall implement its plans to each identified vulnerability in accordance with the report delivered pursuant to Paragraph 7.3 save to the extent directed by TfL in writing.

7.5 The Supplier shall, upon request by TfL, following a Security Incident, carry out such additional security testing over and above the obligations set out in Paragraph 7.2 as TfL requires.

7.6 TfL shall be entitled to send a member of TfL Personnel to witness the conduct of any audit or security tests carried out by or on behalf of the Supplier. The Supplier shall provide TfL with the results of such audits (in a form agreed with TfL in advance) as soon as practicable after the completion of each audit or test.

7.7 In addition to complying with the Requirements, PCI DSS where applicable and other relevant industry standards and Good Industry Practice, the Supplier shall at least once during each twelve (12) month period starting from the Service Commencement Date, engage an appropriately skilled third party to conduct a formal audit of the Services against the then current versions of the following:

(a) the security controls, processes and procedures required pursuant to this Agreement;

(b) the Data Protection Legislation (using BS10012 or another standard as agreed with TfL), where applicable; and

(c) the Security Management Plan,

and shall, within five (5) Working Days of becoming aware of actual or potential security issues which impact or could impact the Services, the Supplier shall inform TfL of each such issue and shall keep TfL up-to-date as the Supplier investigates the nature and

impact of such issue. Within five (5) Working Days of the finalisation of the audit findings, the Supplier shall provide to TfL a copy of all such findings which are relevant to the Services.

7.8 Without prejudice to any other right of audit or access granted to TfL pursuant to this Agreement or at Law, TfL and/or its representatives may carry out such audits in relation to security matters as are reasonably required to assess the Supplier's compliance with the Information Security Management System and the Security Management Plan.

7.9 If any test or audit carried out pursuant to this Paragraph 7 reveals any non-compliance with this Agreement or vulnerability (and, in the case of a TfL audit, TfL has informed the Supplier thereof), the Supplier shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement including the TfL Change Management Process and the Variation Procedure. The Supplier shall implement its plans to remedy each identified vulnerability in accordance with such report save to the extent directed by TfL in writing.

8. SECURITY INCIDENT MANAGEMENT PROCESS

8.1 The Supplier shall, and shall procure that its Sub-contractors shall:

(a) establish, document and share with TfL a process to identify and respond to Security Incidents and mitigate the impact of such Security Incidents on the Services, including in relation to assigning clearly defined roles and responsibilities to specific Supplier Personnel;

(b) record each Security Incident and corresponding severity level in the Supplier's ISMS; and

(c) without limitation to the other provisions of this Agreement, follow TfL's reasonable instructions in relation to the identification and resolution of any Security Incident.

8.2 The Supplier shall notify and ensure TfL is aware as soon as possible and in any event no later than within one (1) hour upon becoming aware of any Security Incident or any potential Security Incident.

8.3 In addition to the requirements in clause 8.2 the Supplier will additionally provide written notice with all relevant details reasonably available of any actual or suspected breach of security in relation to TFL Personal Data including unauthorised or unlawful access or Processing of, or accidental loss, destruction or damage of any Authority Personal Data

8.4 If a Security Incident occurs, the Supplier shall, within the framework of the Security Incident Management Process:

(a) immediately take steps to assess the scope of the Data, user accounts and/or TFL Personal Data compromised or affected including, but not limited to, the amount of Data and/or TfL Personal Data affected;

(b) immediately take the steps necessary to remedy or protect the integrity of the Services against any such Security Incident;

(c) securely collect and preserve evidence, including logs, to support the Security Incident management process described in this Paragraph and share with TfL such evidence via secure channels as requested by TfL;

(d) handle any information pertaining to the Security Incident according to the handling requirements for TfL RESTRICTED information defined in TfL's Information Security Classification Standard;

(e) promptly escalate the Security Incident to a person or governance forum with a level of seniority within the Supplier's organisation as TfL may reasonably require;

(f) as requested by TfL:

(i) provide such information in relation to the Security Incident (including, if necessary, by collating such information from its and its Sub-contractors' systems and the Supplier Personnel);

(ii) provide relevant TfL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Supplier Sites and Supplier Personnel in order to investigate the Security Incident; and

(iii) follow TfL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services; and

(g) as soon as reasonably practicable develop and provide TfL with a copy of its remediation plan for the Security Incident which sets out full details of the steps taken and to be taken by the Supplier to:

(i) correct, make good, reinstate, replace and remediate all deficiencies and vulnerabilities, loss and/or damage to the Service Assets, Data, and/or Services in connection with the Security Incident; and

(ii) perform or re-perform any security tests or alternative tests relating to the security of the Service Assets and/or Services as appropriate and within the timescales specified by TfL, to assure TfL that the Security Incident has been addressed and its effects mitigated,

provided that any such remediation must be implemented in accordance with this Agreement including the TfL Change Management Process and the Variation Procedure. The Supplier shall fully implement and comply with such remediation plan save to the extent directed by TfL in writing

8.5 The Supplier shall provide a detailed report to TfL within two (2) Working Days of the resolution of the Security Incident, such report to detail:

(a) the nature of the Security Incident;

(b) the causes and consequences of the Security Incident;

(c) the actions undertaken and length of time taken by the Supplier to resolve the Security Incident; and

(d) the actions undertaken by the Supplier to prevent recurrence of the Security Incident.

8.6 If there is a suspected security event up to and including a Security Incident, the Supplier shall to the extent requested by the TfL CISO (or any duly authorised delegate):

(a) provide information in relation to the Services which is relevant collating, if necessary, relevant information from Sub-contractors' systems and the Supplier Personnel;

(b) provide relevant TfL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Supplier Sites and Supplier Personnel in order to investigate the security incident; and

(c) follow TfL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services; and

(d) work with TfL to identify any lessons learnt which could mitigate any gaps in process, policy or controls.

and TfL shall reimburse the Supplier's reasonable, demonstrable costs and expenses in relation to the Supplier's compliance with such request.

9. SECURITY LOGGING AND MONITORING

9.1 The Supplier shall ensure that the Security Management Plan sets out its monitoring strategy to monitor its own performance of its obligations under this Schedule. The Supplier shall update its monitoring strategy as necessary throughout the term of this Agreement in response to:

(a) changes to applicable laws, regulations and standards;

(b) changes to Good Industry Practice;

(c) any relevant Operational Changes or Variations and/or associated processes;

(d) any Security Incident; and

(e) any reasonable request by TfL.

9.2 The monitoring strategy should include, as a minimum, processes for monitoring and logging (as appropriate):

(a) networks and host systems to detect attacks originating both on an internal private network or from public networks (e.g. internet);

(b) instances of misuse of the Services, Supplier systems used in the delivery of the Services and access to TfL RESTRICTED Data by TfL Personnel and Supplier Personnel, including attempts at such misuse;

(c) wireless access points to ensure that all wireless networks are secure and no unauthorised access points are available;

(d) Malicious Software on: (i) the Supplier systems used in the delivery of the Services and, (ii) the Services;

(e) access to and movement of TFL RESTRICTED Data, including internal access to such Data; and

(f) traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attempt or actual attack.

9.3 The Supplier shall ensure that access to system logs and monitoring information is strictly restricted to those Supplier Personnel who need to access these items to ensure the delivery and integrity of the Services.

9.4 The Supplier shall ensure that any monitoring process complies with the monitoring strategy developed in accordance with Paragraphs 9.1 and 9.2 and all of its legal and regulatory obligations pursuant to Applicable Law.

9.5 The Supplier shall maintain a log of:

(a) all instances of Supplier Personnel accessing Personal Data;

(b) all Service Recipient, TfL Personnel and Supplier Personnel logon attempts, successful and failed, to the Services or any elements of the Supplier Solution requiring authentication;

(c) all actions taken by Service Recipients, TfL Personnel or Supplier Personnel with administrative privileges;

(d) all instances of accounts being created for Service Recipients, TfL Personnel or Supplier Personnel and their relevant privileges;

(e) all records of formal staff induction or certification required by Supplier Personnel to operate systems and handle TFL RESTRICTED Data (where required);

(f) all instances of accounts for Service Recipients, TfL Personnel, or Supplier Personnel being deleted;

(g) Supplier Personnel system access group memberships in relation to relevant Service Assets;

(h) Service Recipient and group privilege changes against each of the system resources;

(i) unauthorised use of input and output devices and removable media; and

(j) all access to log files and audit systems.

9.6 The logs required in 9.5 above must be raw logs, which are provided in a structured text format and the schema for such logs will need to be provided.

9.7 The Supplier shall implement recording mechanisms to identify TfL Personnel and Supplier Personnel and their actions when cases of misuse are being investigated and shall ensure that any such recording mechanisms are protected against manipulation and disruption.

9.8 The Supplier shall regularly review logs to identify: (i) anomalies; (ii) suspicious activity; and (iii) suspected Security Incidents. The Supplier shall notify TfL of such findings in accordance with Paragraph 8.2

9.9 The Supplier shall provide copies of any log data collected by the Supplier during its delivery of the Services (system audit log data) at TfL's request in a human readable electronic format such as comma-separated value or Microsoft Excel.

10. MALICIOUS SOFTWARE

10.1 The Supplier shall throughout the Term, use the latest versions of anti-malware solutions and software available from an industry accepted vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the IT Services (or as otherwise agreed by the parties).

10.2 Notwithstanding Clause 10.1, if Malicious Software is detected within services provided by the Supplier, the Supplier shall ensure the effect of the Malicious Software is mitigated and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Data, restore the Services to their desired operating efficiency.

10.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause 10.2 shall be borne by the Parties as follows:

(a) by the Supplier if the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier (except where TfL has waived the obligation set out in Clause 10.11) or TfL Data (whilst TfL Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by TfL when provided to the Supplier; and

(b) otherwise by TfL.

11. REMOVABLE MEDIA

11.1 The Supplier may only use Removable Media to support its delivery of the Services if it has obtained prior written consent of TfL and has implemented appropriate controls to ensure that the use of any input or output devices and removable media is restricted strictly to that needed to supply and support delivery of the Services.

11.2 If removable media is approved for use by TfL, the Supplier shall ensure that it deploys suitable anti-virus and anti-malware checking solutions to actively scan for the introduction of Malware onto systems and networks through all Data imports and exports from removable media and that the removable media is encrypted to a suitable standard agreed in advance with TfL in writing.

11.3 The Supplier shall report any loss or interception of Data as a result of the use of removable media to TfL in accordance with Clause 8 and TfL reserves the right in such

instances to rescind its approval in relation to the Supplier's continued use of removable media.

12. MOBILE AND HOME WORKING

12.1 The Supplier may only use offer Mobile and Home working to support its delivery of the Services if it has obtained prior written consent of TfL and has implemented appropriate controls to ensure.

12.2 If such consent is granted but the Supplier does not have a home and mobile policy for Supplier Personnel, TfL's Home and Mobile Working Cyber Security Policy shall apply to the Supplier and its Supplier Personnel.

12.3 If the Supplier has a home and mobile working policy in relation to the Supplier Personnel, the Supplier shall:

(a) ensure through this policy that:

(i) Data is protected and suitably encrypted in line with Cyber Security Policy (see Annex 5), when stored outside of the Supplier Premises;

(ii) Data is protected when accessed, imported or exported through a connection other than one which is accessed at the Supplier Premises; and

(iii) Security Incident management plans acknowledge the increased risk posed by home and mobile working such as theft or loss of Data and TfL Data and/or devices; and

12.4 The Supplier shall report any loss or interception of Data or TfL Data as a result of home or mobile working to TfL in accordance with Clause 8.

13. DISPOSALS

13.1 The Supplier shall not reuse any Service Asset or Removable Media used in the performance of the Services unless such items have been wiped securely in accordance with a TfL agreed standard.

13.2 The Supplier shall securely dispose of and delete Data from Service Assets used for the delivery of the Services to a TfL agreed standard upon the termination or expiry of this Agreement or when such Service Assets are no longer required for the delivery of the Services, whichever is sooner, and documented accordingly.

13.3 The Supplier shall ensure that the disposal of any Service Asset is accurately reflected in the Information Asset Register.

14. SECURITY MANAGEMENT PLAN

14.1 The Outline Security Management Plan as at the Start Date is set out at Annex 1 (*Outline Security Management Plan*).

14.2 The Supplier shall within fifteen (15) Working Days of the Start Date submit to TfL for approval, a draft Security Management Plan which a minimum will:

(a) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the Services comply with this Schedule;

(b) reference and comply with the security requirements set out in Annex 3;

(c) state any other cyber security industry standards over and above those set out in this Schedule which are applicable to the Services;

(d) state all applicable law which relates to the security of the Services; and

(e) how the Supplier will comply with any other security requirements TfL may reasonably request from time to time.

When the Security Management Plan is approved by TfL the approved plan will replace the Outline Security Management Plan in Annex 1.

14.3 The Supplier shall review and update the Security Management Plan at least annually and as required in response to:

(a) changes to the Cyber Security Standards;

(b) emerging changes in Good Industry Practice;

(c) any relevant Operational Change or Variation and/or associated processes;

(d) any new perceived or changed security threats; and

(e) any reasonable request by TfL.

14.4 The Supplier shall submit any amendments to the Security Management Plan for Approval by TfL in accordance with the variation procedure set out in this Agreement

15. INFORMATION SECURITY MANAGEMENT SYSTEM

15.1 The Supplier shall develop, implement, operate, maintain the ISMS and shall within fifteen (15) Working of the Start Date submit a draft ISMS to TfL to assure. The Supplier shall ensure that the ISMS includes the Security Incident Management Process, dealing with, among other matters, Security Incident management.

15.2 The ISMS shall, unless otherwise specified by TfL in writing, be designed to protect all aspects of:

(a) the Services;

(b) all processes associated with the delivery of the Services; and

(c) TfL Sites, the Supplier Solution and any information and Data (including TfL Confidential Information and TfL Data) to the extent used by TfL or the Supplier in connection with this Agreement.

15.3 The Supplier shall make any document referenced in the ISMS available to TfL upon request.

15.4 If the investigation of a Security Incident reveals weaknesses or flaws in the ISMS, then any change to the ISMS to remedy the weakness or flaw shall be submitted to TfL for approval in accordance with the Variation procedure set out in this Agreement for the avoidance of doubt, if a change needs to be made to the ISMS to address an instance of non-compliance with the Security Management Plan or security requirements, the change to the ISMS shall be at no cost to TfL.

15.5 The ISMS will be fully reviewed in accordance with ISO/IEC 27001 by the Supplier at least annually, or from time to time as agreed with TfL, in response to:

(a) changes to Good Industry Practice;

(b) any relevant Operational Changes or Variations or proposed Operational Changes or Variations to the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by TfL.

15.6 The Supplier shall provide the results of such reviews to TfL (together with such related information as TfL may reasonably request) as soon as reasonably practicable after their completion. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that affect the ability to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

16. COMPLIANCE WITH ISO/IEC 27001

16.1 The Supplier shall obtain certification from a UKAS registered organisation of the ISMS to ISO/IEC 27001 for any aspects of the business that is necessary to support the Services. The Supplier shall obtain such certification within twelve (12) months of the Start Date and shall maintain such certification throughout the Term.

16.2 If certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in ISO/IEC 27001 and, the Supplier shall promptly notify TfL of this.

16.3 Without prejudice to any other audit rights set out in this Agreement TfL may carry out, or appoint an independent auditor to carry out, such regular security audits as may be required in accordance with Good Industry Practice in order to ensure that the ISMS maintains compliance with the principles and practices of ISO/IEC27001.

16.4 If on the basis of evidence provided by such audits, TfL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Supplier, then TfL shall notify the Supplier of the same and the Supplier shall, as soon as reasonably practicable, provide TfL with a written plan to remedy each such non-compliance as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement.

17. APPROVED PRODUCTS

17.1 The Supplier shall ensure that all Service Assets providing security enforcing functionality are certified under the CESG Commercial Product Assurance (CPA) Scheme, to the appropriate grade, as defined with Annex 3 "Security Requirements", provided that relevant certified products are available in the market.

17.2 If a product is not assured under the CPA scheme, TfL reserves the right to require bespoke assurance of that product under a recognised scheme such as CESG Tailored Assurance Service (CTAS).

ANNEX 1 – OUTLINE SECURITY MANAGEMENT PLAN/SECURITY MANAGEMENT PLAN

[NOTE TO BIDDERS: This is subject to approval by TfL. This will be updated in accordance with clause 14.]

ANNEX 2 – OUTLINE RISK MANAGEMENT PROCESS

[NOTE TO BIDDERS: This is subject to approval by TfL. Supplier must ensure the following points are covered:

- ***How and when risk assessments are conducted***
- ***Once found, what are the timeframes mitigations of risks once discovered***
- ***Whether vulnerability scans or vulnerability management are to be provided***
- ***The regularity of vulnerability scans and penetration testing***
- ***The type of scans required (credentialed or non-credentialed)***
- ***The output of this service- whether the automated report from the scanning tool or a fully analysed report***
- ***Against what baseline the scans will be performed]***

ANNEX 3 – SECURITY REQUIREMENTS

[Note TfL (CSIRT) – Any additional security requirements to be inserted]

ANNEX 4 – CONFIGURATION MANAGEMENT OF SERVICE ASSETS

[Note TfL (CSIRT) – Any additional security requirements to be inserted]

ANNEX 5 – LIST OF RELEVANT POLICIES

TO BE PROVIDED BY TFL UPON REQUEST

- **Network Security Policy** defines the requirements for securing TfL networks as well as the information and network specific devices on them.
- **System Access Control Policy** defines the requirements for managing user and system account access to applications and technology such as allowing them to sign in to OneLondon or SAP.
- **Cyber Security Incident Management Policy** defines how we will handle cyber security incidents and the requirements for reporting and managing those incidents.
- **Malware Prevention Policy** defines the requirements for helping to prevent malware (malicious software eg computer viruses) from infecting our systems and networks.
- **Security Logging, Monitoring and Audit Policy** details the requirements for security logging and monitoring of access to our technology and data and the audit capabilities.
- **Removable Media Policy** details the requirements for using removable media such as USBs, CDs or portable hard drives.
- **Home and Mobile Working Cyber Security Policy** details the requirements for allowing and supporting secure home and mobile working.
- **Third Party Cyber Security Policy** defines the rules governing how the security of third party custodians of TfL information, technology and third party connections to TfL systems will be ensured.
- **TfL Information Security Classification Standard** details the information security classification scheme covering information and records, in all formats, and the minimum requirements for managing such information
- **10 Steps to Cyber Security -** https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
- **Cyber Essentials Scheme** **https://www.gov.uk/government/publications/cyber-essentials-scheme-overview**

- **Security Patching Standard** details the requirements for applying security-related updates ('security patches') in order to help secure TTL systems and applications in line with the secure builds and configurations policy.

- **Operations Technology Cyber Security Standard** describes the cyber security requirements for operational technology assets throughout their lifecycle