

G-Cloud 12 Call-Off Contract

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

[Part A: Order Form 2](#_TOC_250005)

[Schedule 1: Services 12](#_TOC_250004)

[Schedule 2: Call-Off Contract charges 12](#_TOC_250003)

[Part B: Terms and conditions 13](#_TOC_250002)

Schedule 3: Collaboration agreement 32

Schedule 4: Alternative clauses 44

Schedule 5: Guarantee 49

[Schedule 6: Glossary and interpretations 57](#_TOC_250001)

[Schedule 7: GDPR Information 68](#_TOC_250000)

# Part A: Order Form

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

|  |  |
| --- | --- |
| **Digital Marketplace service ID number** | 455087556578621 |
| **Call-Off Contract reference** | PROJ\_6485 |
| **Call-Off Contract title** | DfE Secondary BACs Service – Fusion Bacsactive-IP |
| **Call-Off Contract description** | * Provision of a Bacs direct Payment service
 |
| **Start date** | Deemed to be effective from 18 July 2022 |
| **Expiry date** | 17 July 2024\*\*This Call-Off Contract is valid for an initial period of 12 months with an option to extend for a further period of up to 12 months (1 year + 1 year).Year 2 is subject to additional DfE internal approvals and is not committed |
| **Call-Off Contract value** | Year 1: up to £34,475 plus VAT Year 2: up to £23,200 plus VAT\*Total contract value: up to £57,675 plus VAT = £69,210 |

|  |  |
| --- | --- |
|  | \* Year 2 subject to additional internal DfE approval |
| **Charging method** | Invoice |
| **Purchase order number** | TBC |

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

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

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

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

|  |  |
| --- | --- |
| **From the Buyer** | Department for EducationCheylesmore House Quinton Road Coventry West Midlands CV1 2WTUnited Kingdom |
| **To the Supplier** | Finastra trading as Accountis Europe Limited 4 Kingdom StreetPaddington London W2 6BDUnited Kingdom orFfordd y Llyn, Parc Menai, Bangor, Gwynedd, LL57 4EZ Company Number: 04407628 |

**Together the ‘Parties’**

### Principal contact details

**For the Buyer:**

Name: **<REDACTED>**

Email: **<REDACTED>**

**For the Supplier:**

Name: **<REDACTED>**

Email: **<REDACTED>**

Phone: **<REDACTED>**

### Call-Off Contract term

|  |  |
| --- | --- |
| **Start date** | This Call-Off Contract is valid for 24 months (12months + 12 months- year 2 subject to additional internal DfE approvals)[The date and number of days or months is subject to clause1.2 in Part B below.] |
| **Ending (termination)** | The notice period for the Supplier needed for Ending the Call- Off Contract is at least 90 Working Days from the date of written notice for undisputed sums (as per clause 18.6).The notice period for the Buyer is a maximum of 30 days from the date of written notice for Ending without cause (as per clause 18.1). |

|  |  |
| --- | --- |
| **Extension period** | This Call-Off Contract can be extended by the Buyer for 1 period of up to 12 months each by giving the Supplier 1 month’s written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.The extension period after 24 months should not exceed the maximum permitted under the Framework Agreement which is 2 periods of up to 12 months each.If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance:<https://www.gov.uk/service-manual/agile-delivery/spend-> [controls-check-if-you-need-approval-to-spend-money-on-a-](https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service) [service](https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service) |

Buyer contractual details

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

|  |  |
| --- | --- |
| **G-Cloud lot** | This Call-Off Contract is for the provision of Services under:* Lot 2: Cloud software
 |
| **G-Cloud services** | The Services to be provided by the Supplier under the above |
| **required** | Lot are listed in Framework Section 2 and outlined below: |
|  | Service Description: 455087556578621 |
|  |  |
|  | Service Description |
| **Additional Services** | N/A |



|  |  |
| --- | --- |
| **Location** | The Services will be delivered remotely as a SaaS and hosted by Supplier. |
| **Quality standards** | The quality standards required for this Call-Off Contract are as detailed in suppliers Gcloud service description |
| **Technical standards:** | The Supplier shall adhere to ISO 27001 (Information Security Management System) and ISO 22301 (Business Continuity Solutions) standards or provide evidence of related practices to satisfy the Buyer.* All user interface components comply with industry usability standards:
	+ Compliance with Web Content Accessibility Guidelines (WCAG) V2.1 to 'AA' Standard
	+ Compliance with ISO 9241-171:2008 (Ergonomics of human-system Interface)
* All user interface components comply with usability regulations:
	+ Compliance with Equality Act 2010
	+ Public Sector Bodies Accessibility Regulations 2018
 |
| **Service level agreement:** | The service level and availability criteria required for this Call- Off Contract are in the Supplier’s Service Definition and Service Description455087556578621-service-definition-doc* Supplier Disaster Recovery Point Objective (RPO) of 30 minutes, and a maximum of 8 hours. Recovery Time Objective (RTO) of 4 hours.
* Supplier service support hours are 08:00 – 18:00 5 days a week (business days) except bank holidays. All year round.
* The standard service level provides availability for 99.5% 7\*24 hours (all days).
 |

|  |  |
| --- | --- |
|  | * Service level response time to be provided by Supplier:
	+ Priority 1 (critical) – target response within 15 minutes, target resolution within 1 hour.
	+ Priority 2 – target response within 30 minutes, target resolution within 24 hours with an update provided within 1 hour
	+ Priority 3 – target response within 1 day, target resolution within 5 working days with an update provided within 2 hours
* Incident Management process: **<REDACTED>**
* **Suppliers’ adherence to Buyer’s requirements**
	+ Supplier will adhere to the requirements set out in the document entitled ‘Secondary Payment Requirements V1.0’ for the duration of this contract term.

**<REDACTED>** |
| **Onboarding** | The Supplier and Buyer shall attend an onboarding meeting and agree the onboarding tasks:* The Supplier will provide access credentials to their service.
* The Supplier will attend a start-up meeting with the representatives of the Buyer.
* The Supplier will provide configuration requirements to the Buyer.
* The Buyer will have quarterly touchpoints with the Suppliers Relationship Manager to review service provision.
 |

|  |  |
| --- | --- |
| **Offboarding** | The offboarding plan for this Call-Off Contract will be prepared by the Supplier and submitted to the Buyer within 10 weeks/months of the contract commencing* The Supplier will ensure upon the exit contract that all Buyer data will be securely transferred back to the Buyer and securely destroyed.
 |
| **Collaboration agreement** | N/A |
| **Limit on Parties’ liability** | If applicable, the annual total liability of either Party for all Property defaults will not exceed £1,000,000The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract TermThe annual total liability for all other defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term. |
| **Insurance** | The insurance(s) required will be:* a minimum insurance period of 1 year following the expiration or Ending of this Call-Off Contract
* Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)]
* employers' liability insurance with a minimum limit of

£5,000,000 or any higher minimum limit required by Law |
| **Force majeure** | A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 28 consecutive days.[This section relates to clause 23.1 in Part B below.] |

|  |  |
| --- | --- |
| **Audit** | The following Framework Agreement audit provisions will be |
|  | incorporated under clause 2.1 of this Call-Off Contract to |
|  | enable the Buyer to carry out audits: |
|  | 7.4 |
|  | 7.5 |
|  | 7.6 |
|  | 7.7 |
|  | 7.8 |
|  | 7.9 |
|  | 7.10 |
|  | 7.11 |
|  | 7.12 |
|  | 7.13 |
| **Buyer’s responsibilities** | The Buyer is responsible for:1. The Buyer will work with the Supplier in order that any required resources and documentation can be made available in order to support the achievement of activities and production of deliverables.
2. Provision of data being processed through Supplier’s service tool.
3. Utilising access credentials in accordance with Buyer and Supplier’s security policies.
4. Attend Supplier contract review sessions.
5. Provide PO and pay invoice.
 |
| **Buyer’s equipment** | N/A |

### Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners** | N/A |

Call-Off Contract charges and payment

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

|  |  |
| --- | --- |
| **Payment method** | The payment method for this Call-Off Contract is BACs |
| **Payment profile** | The payment profile for this Call-Off Contract is a fixed monthly charge which will be paid monthly via BACS for the duration of the contract.” Additional professional services after the initial order will be invoiced monthly in arrears. |
| **Invoice details** | The Supplier will issue electronic invoices monthly in advance. Invoices relating to additional professional services shall be invoiced in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice. |
| **Who and where to send invoices to** | Invoices will be sent to : **<REDACTED>**  |
| **Invoice information required** | All invoices must include:* The correct sum (in £ sterling)
 |
|  | * The correct terms of services/goods supplied
 |
|  | * A unique invoice number
 |
|  | * A valid purchase order number
 |
|  | * Correct Supplier details, date and contact details
 |
|  | * Have been delivered to the nominated address
 |
|  | * Have been delivered in timing in accordance with the contract
 |
| **Invoice frequency** | Invoice will be sent to the Buyer monthly, with the exception of ad-hoc additional professional services which will be invoiced in arrears |

|  |  |
| --- | --- |
| **Call-Off Contract value** | The total value of this Call-Off Contract is : Year 1: up to £34,475 plus VATYear 2: up to £23,200 plus VATTotal contract value: up to £57,675 plus VAT = £69,210 |
| **Call-Off Contract charges**Full breakdown of the Charges is –available at Schedule 2 |

### Additional Buyer terms

|  |  |
| --- | --- |
| **Performance of the Service and Deliverables** | This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:* To provide access to the pre-production environment to enable configuration.
* Supplier to implement solution with the Buyer.
* Supplier to carry out testing with Buyer.
* Supplier to assist in go live.
* Ensure exit arrangements are agreed and offboarding is agreed.
 |
| **Guarantee** | N/A |

|  |  |
| --- | --- |
| **Warranties, representations** | N/A |
| **Supplemental requirements in addition to the Call-Off terms** | N/A |
| **Alternative clauses** | N/A |
| **Buyer specific amendments to/refinements of the Call-Off Contract terms** | In accordance with Call-Off Contract clauses, the Supplier has agreed to unqualified acceptance of the Buyers Special Terms as these will apply to the G-Cloud Call-Off Contract terms – as set out in the DfE Special Terms document at Annex A.The Buyer Supplemental Security clauses shall form part of this Call-Off Contract. |
| **Public Services Network (PSN)** | N/A |
| **Personal Data and Data Subjects** | Annex 1 Schedule 7 is being used |

1. Formation of contract
	1. By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call- Off Contract with the Buyer.
	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.
	3. This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
	4. In cases of any ambiguity or conflict, the affected terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

### Background to the agreement

* 1. The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
	2. The Buyer provided an Order Form for Services to the Supplier.

# Schedule 1: Services

|  |  |  |
| --- | --- | --- |
| **Signed** | Finastra (Accountis Europe Ltd) | Department for Education |
| **Name** | **<REDACTED>** | **<REDACTED>** |
| **Title** | **<REDACTED>** | **<REDACTED>** |
| **Signature** | **<REDACTED>** | **<REDACTED>** |
| **Date** | 02-Aug-2022[**Enter date**] | 03-Aug-2022[**Enter date**] |



#### SCHEDULE OF WORK

|  |  |  |
| --- | --- | --- |
| **Task** | **Output** | **Date Required** |
| Preparation of timetable showing key project dates including implementing test environment | Timetable agreed with DfE. | By 22/07/2022 |

|  |  |  |
| --- | --- | --- |
| Business Requirement Document/ onboarding document to be completed by Finastra | BRD sent by Finastra BRD completed by DfE | By 22/07/2022 |
| Configuration into Supplier service | Supplier system contains DfE configuration details in their system | By 22/07/2022 |
| Configuration into Buyer existing systems with new Supplier interfaces | BC system and interfaces to Finastra | 22/07/22 |
| Build | preproduction system is built | 22/08/22 |
| Test in preproduction environment | System test, UAT complete in PP environment and business sign off | 05/09/22 |
| Build live | Live environment and interfaces built | 07/09/22 |
| Test in live environment | Test payments through to bacs | 09/09/22 |
| Implementation | Implement live system (technical go live) | 16/09/22 |
| Go live | Solution live for business use | 19/09/2022 |
| ELS | Post go live support | 19/09/2022 –23/09/22 |

# Schedule 2: Call-Off Contract charges



**<REDACTED>**

Year 1: up to £34,475 plus VAT Year 2: up to £23,200 plus VAT

**Total contract value: up to £57,675 plus VAT = £69,210**

# Part B: Terms and conditions

### Call-Off Contract Start date and length

* 1. The Supplier must start providing the Services on the date specified in the Order Form.
	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.
	3. The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
	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.

### Incorporation of terms

* 1. The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
* 4.1 (Warranties and representations)
* 4.2 to 4.7 (Liability)
* 4.11 to 4.12 (IR35)
* 5.4 to 5.5 (Force majeure)
* 5.8 (Continuing rights)
* 5.9 to 5.11 (Change of control)
* 5.12 (Fraud)
* 5.13 (Notice of fraud)
* 7.1 to 7.2 (Transparency)
* 8.3 (Order of precedence)
* 8.6 (Relationship)
* 8.9 to 8.11 (Entire agreement)
* 8.12 (Law and jurisdiction)
* 8.13 to 8.14 (Legislative change)
* 8.15 to 8.19 (Bribery and corruption)
* 8.20 to 8.29 (Freedom of Information Act)
* 8.30 to 8.31 (Promoting tax compliance)
* 8.32 to 8.33 (Official Secrets Act)
* 8.34 to 8.37 (Transfer and subcontracting)
* 8.40 to 8.43 (Complaints handling and resolution)
* 8.44 to 8.50 (Conflicts of interest and ethical walls)
* 8.51 to 8.53 (Publicity and branding)
* 8.54 to 8.56 (Equality and diversity)
* 8.59 to 8.60 (Data protection
* 8.64 to 8.65 (Severability)
* 8.66 to 8.69 (Managing disputes and Mediation)
* 8.80 to 8.88 (Confidentiality)
* 8.89 to 8.90 (Waiver and cumulative remedies)
* 8.91 to 8.101 (Corporate Social Responsibility)
* paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
* any audit provisions from the Framework Agreement set out by the Buyer in the Order Form
	1. The Framework Agreement provisions in clause 2.1 will be modified as follows:
		1. a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’
		2. a reference to ‘CCS’ will be a reference to ‘the Buyer’
		3. a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract
	2. The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.
	3. The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause ‘XX’, where ‘XX’ is the Framework Agreement clause number.
	4. When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### Supply of services

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

### Supplier staff

* 1. The Supplier Staff must:
		1. be appropriately experienced, qualified and trained to supply the Services
		2. apply all due skill, care and diligence in faithfully performing those duties
		3. obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
		4. respond to any enquiries about the Services as soon as reasonably possible
		5. if applicable, complete any necessary Supplier Staff vetting as specified by the

Buyer

* 1. 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.
	2. The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
	3. 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. The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
	5. 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.
	6. 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.
	7. 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.

### Due diligence

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

### Business continuity and disaster recovery

* 1. The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.
	2. The Supplier’s business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
	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.

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

* 1. The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier’s delivery of the Services.
	2. The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
	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.
	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.
	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.
	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. All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
	8. The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
	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.
	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.
	11. If there’s an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does, then the Supplier must provide a replacement valid invoice with the response.
	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.

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

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

### Insurance

* 1. The Supplier will maintain the insurances required by the Buyer including those in this clause.
	2. The Supplier will ensure that:
		1. during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
		2. the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit
		3. all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date
		4. all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of

£5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

* 1. If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
	2. If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
		1. a broker's verification of insurance
		2. receipts for the insurance premium
		3. evidence of payment of the latest premiums due
	3. Insurance will not relieve the Supplier of any liabilities under the Framework Agreement, or this Call-Off Contract and the Supplier will:
		1. take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
		2. promptly notify the insurers in writing of any relevant material fact under any Insurances
		3. hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
	4. The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
	5. 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.
	6. The Supplier will be liable for the payment of any:
		1. premiums, which it will pay promptly
		2. excess or deductibles and will not be entitled to recover this from the Buyer

### Confidentiality

* 1. Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

### Intellectual Property Rights

* 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.
	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.
	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.
	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.
	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:
		1. rights granted to the Buyer under this Call-Off Contract
		2. Supplier’s performance of the Services
		3. use by the Buyer of the Services
	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:
		1. modify the relevant part of the Services without reducing its functionality or performance
		2. substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
		3. buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
	7. Clause 11.5 will not apply if the IPR Claim is from:

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

11.7.3 other material provided by the Buyer necessary for the Services

* 1. 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.

### Protection of information

* 1. The Supplier must:
		1. comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data
		2. only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
		3. take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes
	2. The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
		1. providing the Buyer with full details of the complaint or request
		2. complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions
		3. providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
		4. providing the Buyer with any information requested by the Data Subject
	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.

### Buyer data

* 1. The Supplier must not remove any proprietary notices in the Buyer Data.
	2. The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
	3. If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
	4. The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier’s and Buyer’s security policies and all Buyer requirements in the Order Form.
	5. The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
	6. The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
		1. the principles in the Security Policy Framework: <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:

https:/[www.gov.uk/government/publications/government-security-classifications](http://www.gov.uk/government/publications/government-security-classifications)

* + 1. guidance issued by the Centre for Protection of National Infrastructure on Risk Management:

<https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

* + 1. the National Cyber Security Centre’s (NCSC) information risk management guidance:

<https://www.ncsc.gov.uk/collection/risk-management-collection>

* + 1. government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

[https://www.gov.uk/government/publications/technology-code-of-](https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice) [practice/technology-code-of-practice](https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice)

* + 1. the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>
		2. buyer requirements in respect of AI ethical standards
	1. The Buyer will specify any security requirements for this project in the Order Form.
	2. 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.

* 1. 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.
	2. 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.

### Standards and quality

* 1. The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
	2. The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: [https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-](https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice) [of-practice](https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice)
	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.
	4. If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
	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.

### Open source

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

### Security

* 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.

* 1. The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
	2. 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.
	3. Responsibility for costs will be at the:
		1. Supplier’s expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
		2. Buyer’s expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer’s control
	4. The Supplier will immediately notify the Buyer of any breach of security of Buyer’s Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer’s Confidential Information however it may be recorded.
	5. Any system development by the Supplier should also comply with the government’s ‘10 Steps to Cyber Security’ guidance:

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>

* 1. 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.

### Guarantee

* 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:
		1. an executed Guarantee in the form at Schedule 5
		2. a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

### Ending the Call-Off Contract

* 1. The Buyer can End this Call-Off Contract at any time by giving 30 days’ written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier’s obligation to provide the Services will end on the date in the notice.
	2. The Parties agree that the:
		1. Buyer’s right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
		2. Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier’s avoidable costs or Losses
	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.
	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:
		1. a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
		2. any fraud
	5. A Party can End this Call-Off Contract at any time with immediate effect by written notice if:
		1. the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
		2. an Insolvency Event of the other Party happens
		3. the other Party ceases or threatens to cease to carry on the whole or any material part of its business
	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.
	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.

### Consequences of suspension, ending and expiry

* 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.
	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.
	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.
	4. Ending or expiry of this Call-Off Contract will not affect:
		1. any rights, remedies or obligations accrued before its Ending or expiration
		2. the right of either Party to recover any amount outstanding at the time of Ending or expiry
		3. the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
			+ 7 (Payment, VAT and Call-Off Contract charges)
			+ 8 (Recovery of sums due and right of set-off)
			+ 9 (Insurance)
			+ 10 (Confidentiality)
			+ 11 (Intellectual property rights)
			+ 12 (Protection of information)
			+ 13 (Buyer data)
			+ 19 (Consequences of suspension, ending and expiry)
			+ 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
			+ 8.44 to 8.50 (Conflicts of interest and ethical walls)
			+ 8.89 to 8.90 (Waiver and cumulative remedies)
		4. any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires
	5. At the end of the Call-Off Contract Term, the Supplier must promptly:
		1. return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
		2. return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
		3. stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
		4. destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
		5. work with the Buyer on any ongoing work
		6. return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
	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.
	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.

### Notices

* 1. Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.
* Manner of delivery: email
* Deemed time of delivery: 9am on the first Working Day after sending
* Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message
	1. 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).

### Exit plan

* 1. The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
	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.
	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.
	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.
	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.
	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:
		1. the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
		2. there will be no adverse impact on service continuity
		3. there is no vendor lock-in to the Supplier’s Service at exit
		4. it enables the Buyer to meet its obligations under the Technology Code Of Practice
	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.
	8. The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
		1. the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
		2. the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
		3. the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
		4. the testing and assurance strategy for exported Buyer Data
		5. if relevant, TUPE-related activity to comply with the TUPE regulations
		6. any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

### Handover to replacement supplier

* 1. At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
		1. data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier’s possession, power or control
		2. other information reasonably requested by the Buyer
	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.
	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.

### Force majeure

* 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.

### Liability

* 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:
		1. Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form
		2. Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form
		3. Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

### Premises

* 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.
	2. The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.
	3. The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.
	4. This clause does not create a tenancy or exclusive right of occupation.
	5. While on the Buyer’s premises, the Supplier will:
		1. comply with any security requirements at the premises and not do anything to weaken the security of the premises
		2. comply with Buyer requirements for the conduct of personnel
		3. comply with any health and safety measures implemented by the Buyer
		4. immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury
	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.

### Equipment

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

### The Contracts (Rights of Third Parties) Act 1999

* 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.

### Environmental requirements

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

### The Employment Regulations (TUPE)

* 1. If applicable, 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.
	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:
		1. the activities they perform
		2. age
		3. start date
		4. place of work
		5. notice period
		6. redundancy payment entitlement
		7. salary, benefits and pension entitlements
		8. employment status
		9. identity of employer
		10. working arrangements
		11. outstanding liabilities
		12. sickness absence
		13. copies of all relevant employment contracts and related documents
		14. all information required under regulation 11 of TUPE or as reasonably requested by the Buyer
	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.
	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.
	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.
	6. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
		1. its failure to comply with the provisions of this clause
		2. any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
	7. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
	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.

### Additional G-Cloud services

* 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.
	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.

### Collaboration

* 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.
	2. In addition to any obligations under the Collaboration Agreement, the Supplier must:
		1. work proactively and in good faith with each of the Buyer’s contractors
		2. co-operate and share information with the Buyer’s contractors to enable the efficient operation of the Buyer’s ICT services and G-Cloud Services

### Variation process

* 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.
	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.
	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.

### Data Protection Legislation (GDPR)

* 1. Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the

appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Not Used

Schedule 4: Not Used

Schedule 5: Not Used

# Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

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

For the Buyer, Crown Copyright which isn’t available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software. |
| **Buyer** | The contracting authority ordering services as set out in the Order Form. |
| **Buyer Data** | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer. |
| **Buyer Personal Data** | The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract. |
| **Buyer Representative** | The representative appointed by the Buyer under this Call-Off Contract. |

|  |  |
| --- | --- |
| **Buyer Software** | Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services. |
| **Call-Off Contract** | This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement. |
| **Charges** | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract. |
| **Collaboration Agreement** | An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer’s Services and to ensure that the Buyer receives end-to-end services across its IT estate. |
| **Commercially Sensitive Information** | Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive. |
| **Confidential Information** | Data, Personal Data and any information, which may include (but isn’t limited to) any:* information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above
* other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
 |
| **Control** | ‘Control’ as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly. |
| **Controller** | Takes the meaning given in the GDPR. |
| **Crown** | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf. |

|  |  |
| --- | --- |
| **Data Loss Event** | Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach. |
| **Data Protection Impact Assessment (DPIA)** | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| **Data Protection Legislation (DPL)** | Data Protection Legislation means:1. the GDPR, the LED and any applicable national implementing Laws as amended from time to time
2. the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy
3. all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
 |
| **Data Subject** | Takes the meaning given in the GDPR |
| **Default** | Default is any:* breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)
* other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract

Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer. |
| **Deliverable(s)** | The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract. |
| **Digital Marketplace** | The government marketplace where Services are available for Buyers to buy. ([https://www.digitalmarketplace.service.gov.uk](https://www.digitalmarketplace.service.gov.uk/)/) |
| **DPA 2018** | Data Protection Act 2018. |
| **Employment Regulations** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) (‘TUPE’) which implements the Acquired Rights Directive. |
| **End** | Means to terminate; and Ended and Ending are construed accordingly. |

|  |  |
| --- | --- |
| **Environmental Information Regulations or EIR** | The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations. |
| **Equipment** | The Supplier’s hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract. |
| **ESI Reference Number** | The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool. |
| **Employment Status Indicator test tool or ESI tool** | The HMRC Employment Status Indicator test tool. The most up-to- date version must be used. At the time of drafting the tool may be found here:<https://www.gov.uk/guidance/check-employment-status-for-tax> |
| **Expiry Date** | The expiry date of this Call-Off Contract in the Order Form. |
| **Force Majeure** | A force Majeure event means anything affecting either Party's performance of their obligations arising from any:* acts, events or omissions beyond the reasonable control of the affected Party
* riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare
* acts of government, local government or Regulatory

Bodies* fire, flood or disaster and any failure or shortage of power or fuel
* industrial dispute affecting a third party for which a substitute third party isn’t reasonably available

The following do not constitute a Force Majeure event:* any industrial dispute about the Supplier, its staff, or failure in the Supplier’s (or a Subcontractor's) supply chain
* any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure
* the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into
* any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
 |
| **Former Supplier** | A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor). |

|  |  |
| --- | --- |
| **Framework Agreement** | The clauses of framework agreement RM1557.12 together with the Framework Schedules. |
| **Fraud** | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown. |
| **Freedom of Information Act or FoIA** | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation. |
| **G-Cloud Services** | The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement. |
| **GDPR** | General Data Protection Regulation (Regulation (EU) 2016/679) |
| **Good Industry Practice** | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |
| **Government Procurement Card** | The government’s preferred method of purchasing and payment for low value goods or services. |
| **Guarantee** | The guarantee described in Schedule 5. |
| **Guidance** | Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence. |
| **Implementation Plan** | The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding. |
| **Indicative test** | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6. |

|  |  |
| --- | --- |
| **Information** | Has the meaning given under section 84 of the Freedom of Information Act 2000. |
| **Information security management system** | The information security management system and process developed by the Supplier in accordance with clause 16.1. |
| **Inside IR35** | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool. |
| **Insolvency event** | Can be:* a voluntary arrangement
* a winding-up petition
* the appointment of a receiver or administrator
* an unresolved statutory demand
* a Schedule A1 moratorium
 |
| **Intellectual Property Rights or IPR** | Intellectual Property Rights are:* copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information
* applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction
* all other rights having equivalent or similar effect in any country or jurisdiction
 |
| **Intermediary** | For the purposes of the IR35 rules an intermediary can be:* the supplier's own limited company
* a service or a personal service company
* a partnership

It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). |
| **IPR claim** | As set out in clause 11.5. |
| **IR35** | IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary. |
| **IR35 assessment** | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35. |

|  |  |
| --- | --- |
| **Know-How** | All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier’s or CCS’s possession before the Start date. |
| **Law** | Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply. |
| **LED** | Law Enforcement Directive (EU) 2016/680. |
| **Loss** | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly. |
| **Lot** | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly. |
| **Malicious Software** | Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence. |
| **Management Charge** | The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract. |
| **Management Information** | The management information specified in Framework Agreement section 6 (What you report to CCS). |
| **Material Breach** | Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract. |
| **Ministry of Justice Code** | The Ministry of Justice’s Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000. |

|  |  |
| --- | --- |
| **New Fair Deal** | The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended. |
| **Order** | An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes. |
| **Order Form** | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services. |
| **Ordered G-Cloud Services** | G-Cloud Services which are the subject of an order by the Buyer. |
| **Outside IR35** | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool. |
| **Party** | The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly. |
| **Personal Data** | Takes the meaning given in the GDPR. |
| **Personal Data Breach** | Takes the meaning given in the GDPR. |
| **Processing** | Takes the meaning given in the GDPR. |
| **Processor** | Takes the meaning given in the GDPR. |
| **Prohibited act** | To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:* induce that person to perform improperly a relevant function or activity
* reward that person for improper performance of a relevant function or activity
* commit any offence:
	+ under the Bribery Act 2010
	+ under legislation creating offences concerning Fraud
	+ at common Law concerning Fraud
	+ committing or attempting or conspiring to commit Fraud
 |
| **Project Specific IPRs** | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical |

|  |  |
| --- | --- |
|  | documentation and schema but not including the Supplier’s Background IPRs. |
| **Property** | Assets and property including technical infrastructure, IPRs and equipment. |
| **Protective Measures** | Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it. |
| **PSN or Public Services Network** | The Public Services Network (PSN) is the government’s high- performance network which helps public sector organisations work together, reduce duplication and share resources. |
| **Regulatory body or bodies** | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract. |
| **Relevant person** | Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body. |
| **Relevant Transfer** | A transfer of employment to which the employment regulations applies. |
| **Replacement Services** | Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party. |
| **Replacement supplier** | Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer). |
| **Security management plan** | The Supplier's security management plan developed by the Supplier in accordance with clause 16.1. |
| **Services** | The services ordered by the Buyer as set out in the Order Form. |
| **Service data** | Data that is owned or managed by the Buyer and used for the G- Cloud Services, including backup data. |

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

|  |  |
| --- | --- |
| **Term** | The term of this Call-Off Contract as set out in the Order Form. |
| **Variation** | This has the meaning given to it in clause 32 (Variation process). |
| **Working Days** | Any day other than a Saturday, Sunday or public holiday in England and Wales. |
| **Year** | A contract year. |

# Schedule 7: GDPR Information

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

### Annex 1: Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

* 1. The contact details of the Buyer’s Data Protection Officer are : **<REDACTED>**
	2. The contact details of the Supplier’s Data Protection Officer are: privacy@finastra.com
	3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
	4. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| Description | Details |
| Identity of the Controller and Processor | The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller, and the Contractor is the Processor in accordance with Clause 17.1. |
| Subject matter of the processing | The Buyer submits BACS payment files into the Supplier’s payment platform |
| Duration of the processing | Duration of the Agreement |
| Nature and purposes of the processing | Payment file processing via BACS;* processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
* processing is necessary for compliance with a legal obligation to which DfE is subject;
* processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in DfE;
* processing is necessary, and records need to be kept for the accounting of financial payments made to Institutions/Suppliers;
 |
| Type of Personal Data |  |

|  |  |
| --- | --- |
|  | Payments can be made to organisations, Sole Traders and individuals. In the case of Sole Traders and individuals the ‘Bank Account Name’ processed may contain the name of a person (along with their bank account details).DfE Finance staff setup as users of the system will need to have their name, email address and role held in the system. |
| Categories of Data Subject | Categories of personal data related to payments could be ‘names of individuals’ if it is included in the bank account name.For DfE staff using the system categories are names, email address and role.No *special category data* is required to be held. |
| Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | All records to be returned to DfE as they must be retained for a minimum of 7 years and must be available for reporting purposes |
| Permitted subcontractors | N/A |

## Annex 2: Joint Controller Agreement (Not Used)

**ANNEX A**

**Library of Clauses: Departmental Security Standards**

## DfE - Departmental Security Requirements

#### Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement the other definitions in the Contract:

|  |  |
| --- | --- |
| “BPSS”“Baseline Personnel Security Standard” | the Government’s HMG Baseline Personal Security Standard. Further information can be found at:[https://www.gov.uk/government/publications/govern-](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard) [ment-baseline-personnel-security-standard](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard) |
| “CCSC”“Certified Cyber Security Consultancy” | is the National Cyber Security Centre’s (NCSC) ap- proach to assessing the services provided by con- sultancies and confirming that they meet NCSC's standards.See website:[https://www.ncsc.gov.uk/scheme/certified-cyber-](https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy) [consultancy](https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy) |
| “CCP”“Certified Professional” | is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website:[https://www.ncsc.gov.uk/information/about-certified-](https://www.ncsc.gov.uk/information/about-certified-professional-scheme) [professional-scheme](https://www.ncsc.gov.uk/information/about-certified-professional-scheme) |
| “CPA”“Commercial Product Assurance”[formerly called “CESG Product Assurance”] | is an ‘information assurance scheme’ which evalu- ates commercial off the shelf (COTS) products and their developers against published security and de- velopment standards. See website: [https://www.ncsc.gov.uk/scheme/commercial-prod-](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa) [uct-assurance-cpa](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa) |
| “Cyber Essentials” “Cyber Essentials Plus” | Cyber Essentials is the government backed, indus- try supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers:[https://www.cyberessentials.ncsc.gov.uk/getting-](https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body) [certified/#what-is-an-accreditation-body](https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body) |

|  |  |
| --- | --- |
| “Data”“Data Controller”“Data Protection Officer” “Data Processor” “Personal Data”“Personal Data requiring Sensitive Processing”“Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Legislation |
| "Buyer’s Data" “Buyer’s Information” | is any data or information owned or retained in order to meet departmental business objectives and tasks, including:1. any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:
	1. supplied to the Supplier by or on behalf of the Buyer; or
	2. which the Supplier is required to generate, process, store or transmit pursuant to this Con- tract; or
2. any Personal Data for which the Buyer is the Data Controller;
 |
| “Departmental Security Standards” | the Buyer’s security policy or any standards, proce- dures, process or specification for security that the Supplier is required to deliver. |
| “Digital Marketplace / G-Cloud” | the Digital Marketplace is the online framework for identifying and procuring cloud technology and peo- ple for digital projects. |
| “End User Devices” | the personal computer or consumer devices that store or process information. |
| “Good Industry Standard” “Industry Good Standard” | the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be ex- pected from a leading company within the relevant industry or business sector. |
| “GSC”“GSCP” | the Government Security Classification Policy which establishes the rules for classifying HMG infor- mation. The policy is available at: [https://www.gov.uk/government/publications/govern-](https://www.gov.uk/government/publications/government-security-classifications) [ment-security-classifications](https://www.gov.uk/government/publications/government-security-classifications) |
| “HMG” | Her Majesty’s Government |
| “ICT” | Information and Communications Technology (ICT) and is used as an extended synonym for information |

|  |  |
| --- | --- |
|  | technology (IT), used to describe the bringing to- gether of enabling technologies used to deliver the end-to-end solution |
| “ISO/IEC 27001” “ISO 27001” | is the International Standard for Information Security Management Systems Requirements |
| “ISO/IEC 27002” “ISO 27002” | is the International Standard describing the Code of Practice for Information Security Controls. |
| “ISO 22301” | is the International Standard describing for Business Continuity |
| “IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” “Penetration Testing” | an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availabil- ity of information held on that IT system. |
| “Need-to-Know” | the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties. |
| “NCSC” | the National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is [https://www.ncsc.gov.uk](https://www.ncsc.gov.uk/) |
| “OFFICIAL”“OFFICIAL-SENSITIVE” | the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP).the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP. |
| “RBAC”“Role Based Access Control” | Role Based Access Control, a method of restricting a person’s or process’ access to information de- pending on the role or functions assigned to them. |
| “Storage Area Network” “SAN” | an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically con- nected storage. |
| “Secure Sanitisation” | the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruc- tion to an acceptable level.NCSC Guidance can be found at: [https://www.ncsc.gov.uk/guidance/secure-sanitisa-](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media) [tion-storage-media](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)The disposal of physical documents and hardcopy materials advice can be found at: <https://www.cpni.gov.uk/secure-destruction-0> |

|  |  |
| --- | --- |
| “Security and Information Risk Advisor” “CCP SIRA”“SIRA” | the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Profes- sional (CCP) Scheme. See also:[https://www.ncsc.gov.uk/articles/about-certified-pro-](https://www.ncsc.gov.uk/articles/about-certified-professional-scheme) [fessional-scheme](https://www.ncsc.gov.uk/articles/about-certified-professional-scheme) |
| “Senior Information Risk Owner” “SIRO” | the Senior Information Risk Owner (SIRO) responsi- ble on behalf of the DfE Accounting Officer for over- seeing the management of information risk across the organisation. This includes its executive agen- cies, arm’s length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties. |
| “SPF”“HMG Security Policy Framework” | the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Gov- ernment’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, effi- ciently and securely. [https://www.gov.uk/govern-](https://www.gov.uk/government/publications/security-policy-framework) [ment/publications/security-policy-framework](https://www.gov.uk/government/publications/security-policy-framework) |
| "Supplier Staff" | all directors, officers, employees, agents, consult- ants, and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier’s obligations under the Contract. |

* 1. **Operative Provisions** The Supplier shall be aware of and comply the relevant [HMG security policy framework](https://www.gov.uk/government/publications/security-policy-framework), [NCSC guidelines](https://www.ncsc.gov.uk/section/advice-guidance/all-topics) and where applicable Depart- mental Security Standards which include but are not constrained to the following paragraphs.
	2. Where the Supplier will provide products or Services or otherwise handle infor- mation at OFFICIAL for the Buyer, the requirements of [Cabinet Office Procurement](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) [Policy Note – Use of Cyber Essentials Scheme certification](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) - [Action Note 09/14](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) dated 25 May 2016, or any subsequent updated document, are mandated, namely that “contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract”. The certification scope shall be relevant to the Ser- vices supplied to, or on behalf of, the Buyer.
	3. Where paragraph 2.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the Services sup- plied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the appli- cation of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

* 1. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer’s Data being handled in the course of providing the Services and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer’s Data).
	2. Buyer’s Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Supplier’s or sub-contractor’s own IT equipment to protect the Buyer’s Data and enable the data to be identified and se- curely deleted when required in line with paragraph 2.14.
	3. The Supplier shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.
	4. The Supplier shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Buyer’s Data. This policy must include appropriate segregation of duties and if ap- plicable role-based access controls (RBAC). User credentials that give access to Buyer’s Data or systems shall be considered to be sensitive data and must be pro- tected accordingly.
	5. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer’s Data, including but not limited to:
		+ physical security controls;
		+ good industry standard policies and processes;
		+ malware protection;
		+ boundary access controls including firewalls, application gateways, etc;
		+ maintenance and use of fully supported software packages in accordance with vendor recommendations;
		+ use of secure device configuration and builds;
		+ software updates and patching regimes including malware signatures, for oper- ating systems, network devices, applications and services;
		+ user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
		+ any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department’s logging and auditing requirements, plus logs shall be:
			- retained and protected from tampering for a minimum period of six months;
			- made available to the department on request.
	6. The Supplier shall ensure that any Buyer’s Data (including email) transmitted over any public network (including the Internet, mobile networks or unprotected enter- prise network) or to a mobile device shall be encrypted when transmitted.
	7. The Supplier shall ensure that any Buyer’s Data which resides on a mobile, remova- ble or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification pro- cess agreed with the Buyer except where the Buyer has given its prior written con- sent to an alternative arrangement.
	8. The Supplier shall ensure that any device which is used to process Buyer’s Data meets all of the security requirements set out in the NCSC End User Devices Plat- form Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security> and [https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-se-](https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles) [curity-principles](https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles).
	9. Whilst in the Supplier’s care all removable media and hardcopy paper documents containing Buyer’s Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using ei- ther a cross-cut shredder or a professional secure disposal organisation.

The term ‘lock and key’ is defined as: “securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user’s sole control and to which they hold the keys”.

* 1. When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer’s Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term ‘under cover’ means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

* 1. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or re- sulting from provision of the Services shall not be considered as the Supplier’s as- sets and must be returned to the Buyer and written assurance obtained from an ap- propriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier’s organisation in line with para- graph 2.15.
	2. In the event of termination, equipment failure or obsolescence, all Buyer’s Data and Buyer’s Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC-approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-con- tractor protects) the Buyer’s Information and Buyer’s Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

* 1. Access by Supplier Staff to Buyer’s Data, including user credentials, shall be con- fined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Se- curity Vetting clearance as required by the Buyer. All Supplier Staff must complete this process before access to Buyer’s Data is permitted. [Any Supplier Staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact].
	2. All Supplier Staff who handle Buyer’s Data shall have annual awareness training in protecting information.
	3. Notwithstanding any other provisions as to business continuity and disaster recov- ery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the Services delivered. If an ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant business conti- nuity arrangements and processes including IT disaster recovery plans and proce- dures. This must include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, in- cluding required actions.
	4. Any suspected or actual breach of the confidentiality, integrity or availability of Buyer’s Data, including user credentials, used or handled in the course of providing the Services shall be recorded as an incident. This includes any non-compliance with the Departmental Security Standards and these provisions, or other security standards pertaining to the solution.

Security Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the Sup- plier must provide an explanation about the delay.

Security Incidents shall be reported through the Buyer’s nominated system or ser- vice owner.

Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

* 1. The Supplier shall ensure that any IT systems and hosting environments that are used to handle, store or process Buyer’s Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go- live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modifi- cation or redaction and all necessary remedial work carried out within the vulnerabil- ity remediation timeframes and SLA requirements. In the event of significant secu- rity issues being identified, a follow up remediation test may be required.
	2. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process or store Buyer’s Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.
	3. The Buyer reserves the right to audit the Supplier or sub-contractors providing the Services within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the Ser- vices being supplied and the Supplier’s, and any sub-contractors’, compliance with the paragraphs contained in this Schedule.
	4. The Supplier and sub-contractors shall undergo appropriate security assurance ac- tivities and shall provide appropriate evidence including the production of the neces- sary security documentation as determined by the Buyer. This will include obtaining any necessary professional security resources required to support the Supplier’s and sub-contractor’s security assurance activities such as: a Security and Infor- mation Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.
	5. Where the Supplier is delivering an ICT solution to the Buyer they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Buyer’s Policy. The Supplier will provide the Buyer with evidence of compliance for the solutions and services to be delivered. The Buyer’s expectation is that the Sup- plier shall provide written evidence of:
* Compliance with HMG Minimum Cyber Security Standard.
* Any existing security assurance for the Services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
* Any existing HMG security accreditations or assurance that are still valid includ- ing: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
* Documented progress in achieving any security assurance or accreditation ac- tivities including whether documentation has been produced and submitted. The

Supplier shall provide details of who the awarding body or organisation will be and date expected.

* 1. The Supplier shall contractually enforce all the Departmental Security Standards and these provisions onto any third-party suppliers, sub-contractors or partners who could potentially access Buyer’s Data in the course of providing the Services.
	2. HSMs (or virtual HSMs in the cloud) must be used to store cryptographic keys and support associated cryptographic functions.
	3. The supplier’s software development lifecycle must include appropriate security as- sessments and coding standards to minimise the potential of the occurrence of soft- ware vulnerabilities. This must include security testing during and post develop- ment phases. Code/Application updates must be made under change control and include independent third-party review of code as a required process as matter of routine.
	4. To support the DfE's departmental security assurance process, the supplier must provide details and a mapping of how their solution/service's security controls sat- isfy, meet or exceed the NCSC and/or UK government requirements set out in (as a minimum):
1. **The Minimum Cyber Security Standard** 25 June 2018 - https://[www.gov.uk/government/publications/the-minimum-cyber-security-stand-](http://www.gov.uk/government/publications/the-minimum-cyber-security-stand-) ard/the-minimum-cyber-security-standard
2. **Cloud Security Principles** 17 November 2018 - https:/[/www.ncsc.g](http://www.ncsc.gov.uk/collec-)o[v.uk/collec-](http://www.ncsc.gov.uk/collec-) tion/cloud-security/implementing-the-cloud-security-principles
3. **Security Design Principles for Digital Services** - https://[www.ncsc.gov.uk/col-](http://www.ncsc.gov.uk/col-) lection/cyber-security-design-principles
	1. The supplier’s system must have a protective monitoring mechanism in place and appropriate processes to monitor, react and notify designated roles upon detection of potential security breach events.
	2. The proposed solution must implement current, strong cryptographic methods.
	3. Strong ciphers must be utilised, and key management process must be docu- mented.
	4. The solution must not use mechanisms, configurations or components for any user authentication, credential, and data transfer that are known to be weak and/or have vulnerabilities (e.g. TLS 1.1).
	5. Certificates must not be self-signed and come from established and reliable inde- pendent CAs (Certificate Authorities).
	6. A sufficient and appropriate level of technical, procedural, and physical controls must be in place so that a malicious or compromised user of the service must not be able to affect the service or data of another.
	7. The Supplier must operate effective mechanisms and processes to manage vulner- abilities, security, and risks. This supplier must also work with the DfE to manage risks and vulnerabilities to the DfE environment, as part of a security working group/forum.
	8. The supplier must remediate, mitigate or otherwise address vulnerabilities to reduce those above a severity of Medium and above to within the risk appetite of DFE (which is Low and below).
	9. The SLA (Service Level Agreement) for the remediation and mitigation of discov- ered vulnerabilities in accordance with their severity must be in completed within the following timeframes (from the point of identification) or sooner. The information for- mat is Vulnerability Severity followed by the Resolution Timeframe.
4. Critical & Above: 48 hours.
5. Important & High: 2-5 days.
6. Moderate & Medium: 5-10 days.
7. Low: 10-28 days.
8. Informational: At the next suitable scheduled maintenance cycle.
	1. The supplier must help facilitate and support the DfE security assurance processes by providing the information it needs to assure the supplier’s system(s). The sup- plier must provide information about the systems and organisation to allow DfE to assess any risk to their payment continuity and security. The supplier must provide design and operational documentation, diagrams, artefacts, etc. to cover, as a mini- mum, the following areas and the interactions and relationships between them::
9. Business Functions.
10. Information Assets & data footprint
11. IT & Technology - Hardware, Software, Applications
12. Personnel & user groups
13. Services utilised and relied on
14. (Main) Processes & procedures to implement policies
	1. Remote access must only be provided to authorised personnel, with the appropriate level of access conformant with the principle of least privilege, be timebound, and formally registered, monitored and periodically reviewed under change control.

\*\*\*End of Security Requirements Clause\*\*\*

.

* 1. The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:
		+ physical security controls;
		+ good industry standard policies and processes;
		+ malware protection;
		+ boundary access controls including firewalls, application gateways, etc;
		+ maintenance and use of fully supported software packages in accordance with vendor recommendations;
		+ use of secure device configuration and builds;
		+ software updates and patching regimes including malware signatures, for oper- ating systems, network devices, applications and services;
		+ user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
		+ any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department’s logging and auditing requirements, plus logs shall be:
			- retained and protected from tampering for a minimum period of six months;
			- made available to the department on request.
	2. The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected en- terprise network) or to a mobile device shall be encrypted when transmitted.
	3. The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certifica- tion process agreed with the department except where the department has given its prior written consent to an alternative arrangement.
	4. The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security> and [https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-se-](https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles) [curity-principles](https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles).
	5. Whilst in the Contractor’s care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term ‘lock and key’ is defined as: “securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user’s sole control and to which they hold the keys”.

* 1. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term ‘under cover’ means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

* 1. In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be con- sidered as the supplier’s assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.
	2. In the event of termination, equipment failure or obsolescence, all Departmental in- formation and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically re- turned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department’s information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

* 1. Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appro- priate National Security Vetting clearance as required by the Department. All Con- tractor or sub-contractor staff who have access to Departmental Data must complete this process before access to Departmental Data is permitted. Any Contractor or sub- contractor staff who will be in contact with children or vulnerable adults must, in addi- tion to any security clearance, have successfully undergone an Enhanced DBS (Dis- closure and Barring Service) check prior to any contact.
	2. All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.
	3. The Contractor shall, as a minimum, have in place robust Business Continuity ar- rangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services deliv- ered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should in- clude evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
	4. Any suspected or actual breach of the confidentiality, integrity or availability of De- partmental Data, including user credentials, used or handled in the course of provid- ing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Stand- ards pertaining to the solution.

Any breach of the confidentiality, integrity or availability of Departmental Data (**Breach/Breaches**) shall be reported to the department without undue delay but always within 36 hours of discovery. If incident reporting has been delayed by more than 36 hours, the contractor should provide an explanation about the delay.

Breaches shall be reported through the department’s nominated system or service owner.

Breaches shall be investigated by the contractor with outcomes being notified to the Department.

* 1. The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go- live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
	2. The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contrac- tor shall not go ahead with any such proposal without the prior written agreement from the Department.
	3. The Department reserves the right to audit the Contractor not more than once per annum within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor’s, and any sub-contractors’, compliance with the clauses contained in this Section. The Contractor will co-operate and provide assis- tance at Department cost (such co-operation including the provision of any reports provided to the Contractor by sub-contractors where available and where the Con- tractor is permitted to disclose those to the Department).
	4. The Contractor shall undergo appropriate internal security assurance activities and shall provide appropriate evidence relating to itself and sub-contractors including the production of the necessary security documentation as determined by the department such as completing the DfE Security Assurance Model (DSAM) process or the Busi- ness Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor’s and sub-contrac- tor’s security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Cer- tified Cyber Professional (CCP) schemes. The DfE agrees that the costs to support these security assurance activities are chargeable and the pricing will be based on the SFIA rate, and the activities and prices will be agreed in advance between both parties.
	5. Where the Contractor is delivering an ICT solution to the Department they shall de- sign and deliver solutions and services that are compliant with the HMG Security Pol- icy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department’s ex- pectation is that the Contractor shall provide written evidence of:
* Compliance with HMG Minimum Cyber Security Standard.
* Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
* Any existing HMG security accreditations or assurance that are still valid includ- ing: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
* Documented progress in achieving any security assurance or accreditation activ- ities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.
	1. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who have access to Departmental Data in the course of providing this service before access to Departmental Data is provided or permitted.

\*\*\*End of Department’s Security Standards Clause\*\*\*

**ANNEX B**

**Supplier terms and conditions : <REDACTED>**