G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

G-Cloud 14 Call-Off Contract

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.

Platform service ID number	426303922263495
Call-Off Contract reference	C373184
Call-Off Contract title	Org Design Software as a Service (SaaS)
Call-Off Contract description	SaaS platform to manage workforce data. For use by DHSC, NHSE, and any other third parties whatsoever that the Buyer may designate.
Start date	19th September 2025
Expiry date	18th September 2028
Call-Off Contract value	A 3-year term = [redacted]. See breakdown in Schedule 2. An option to extend for 1 year
Charging method	Invoicing for professional service elements as set out in Payment Profile section below

	Licensing to be invoiced once per annum, in advance.
Purchase order number	To be provided by the Buyer following contract signature.

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

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 Services 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 of Health and Social Care 39 Victoria Street London United Kingdom SW1H 0EU

To the Supplier	Orgvue Limited Telephone: [redacted] 100 Cheapside London EC2V 6DT United Kingdom Company number: [redacted]
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Commercial Manager
Name: [redacted]
Email: [redacted]
Phone: [redacted]

For the Supplier:

Title: Director, Public Sector
Name: [redacted]
Email: [redacted]
Phone: [redacted]

Call-Off Contract term

Start date	This Call-Off Contract Starts on **19th September 2025** and is valid for 36 months.
Ending (termination)	The parties acknowledge and agree that clauses 18.1 and 18.2 are only applicable to the activation services and additional professional services, and do not apply to the Orgvue subscription.
Extension period	An option to extend for 1 year

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 ● Lot 3: Cloud support
G-Cloud Services	The Services to be provided by the Supplier under the

required	above Lot are listed in Framework Schedule 4 and outlined below: ● **Orgvue cloud software subscription** Service ID 426 303 922 263 495 ● **Orgvue cloud support** Service ID 453 227 898 661 002  Orgview Ltd_service-definition Link: https://redirect.contractawardservice.crowncommercial.gov.uk/service/426303922263495/version/14
Additional Services	As set out in Schedule 1, with notes in that schedule on how some of those requirements are met.  Specification of Requirement.pdf
Location	Unless otherwise agreed in writing by both Parties, all services will be conducted at Orgvue Limited's office or at the buyer's offices in central London (Wellington House and Victoria Street.)
Quality Standards	Orgvue Limited to provide all Quality Management measures that is relevant to their ISO/IEC 27001 certification.
Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are: • Security certificate: ISO/IEC27001: Yes • ISO 9001: No • Cyber Essential Plus certification: No • Certified Security Testing Professional (CSTP) certified test team: No • Certified Application Security Tester (CAST) certified test

	team: No • CREST accreditation: Yes The technical standards used as a requirement for this Call-Off Contract are The Supplier shall maintain compliance with ISO 27001:2013. The Government Technology Code of Practice https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice The Government Service Standard (where applicable) https://www.gov.uk/service-manual/service-standard The Supplier shall maintain compliance with ISO 27001:2013 or equivalent and shall also ensure that any third parties used by it in the course of the service provision and deemed critical to the service, shall adopt a systematic approach to managing information so that it remains secure. Full IT Health Check to be undertaken yearly with Web Application testing undertaken annually with visibility of test scopes, results and remediation plans.
Service level agreement:	The service level and availability criteria required for this Call-Off Contract are set out in the supplier's service definition. All projects and programmes will be subject to the approval of a formal quote or Statement of Work issued by the Supplier to be agreed and signed off by the Buyer prior to work commencing.
Onboarding	The onboarding plan for this Call-Off Contract is defined in the Service Definition for service ID 426303922263495

Offboarding	The offboarding plan for this Call-Off Contract is defined in the Service Definition for service ID 426303922263495

Collaboration agreement	Not applicable.
Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £500,000 per year. The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed £500,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other Defaults will not exceed the greater of £500,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).
Insurance	The Supplier insurance(s) required will be: Professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000); Public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000); and Employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).
Buyer's responsibilities	Not Applicable

Buyer's equipment	Not Applicable

Supplier's information

Subcontractors or partners	The following is a list of the Supplier's Subcontractors or Partners • [redacted] [redacted] [redacted] [redacted]

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 to: Bank: [redacted] Sort Code: [redacted] Account: [redacted] Account Name: Orgvue Limited

Payment profile	The payment profile for this Call-Off Contract is as follows: • Licences: Annual Payment in advance • Activation, fixed price: payable on commencement of this Call-Off Contract. • OD configuration & upskills and Tracking & Monitoring configuration & upskill professional services, time and materials: at the end of each calendar month based on the number of hours incurred. • Success Plan, fixed price: payable at the start of each year. Any travel and subsistence costs for travel outside of central London: Invoiced at cost, monthly in arrears. In line with DHSC travel policy; travel costs not to be incurred without prior confirmation and approval, which approval shall not be unreasonably withheld.
Invoice details	The Supplier will issue an electronic invoice for year one licences in advance, and on delivery in-year for the following services: • Activation, • OD configuration & upskill services, • Tracking & Monitoring configuration & upskill services. • Silver success package The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
Who and where to send invoices to	All invoices to be sent to DHSC Finance Operations team at the [redacted] email address and also CC in [redacted]

Invoice information required	All invoices must include a valid Purchase Order and confirmation of services delivered which can be receipted against. The contract reference number **C373184** must be included.
Invoice frequency	Invoices will be sent to the Buyer on satisfactory receipt of the services at agreed timeframes. Invoices for the licences will be sent to the buyer annually in advance. For years two and three, invoices will be sent on the anniversary of the year one invoice.
Call-Off Contract value	The total value of this Call-Off Contract is [redacted].
Call-Off Contract charges	The breakdown of the Charges is set out year by year in Schedule 2 based on: **Product** **Price** [redacted] Silver success package p/a [redacted]

	[redacted] to constitute Tracking and Monitoring configuration and upskill services and a maximum of [redacted] (time & materials based) to constitute Org Modelling Workflow Configuration and Training services. Total Contract Value (Maximum Price for 3 years, 2 years SWP) [redacted] **Orgvue Rate Card Rates (***indicative, please see G-Cloud pricing attached for fixed prices at all SFIA levels)* **Role*** **Day Rate** [redacted] OrgVue-pricing-document-Rate Card.pdf **Note: Optional service to be confirmed by the buyer in writing. This is only to be used to price a milestone as no payment for resource is permitted under a G-Cloud contract.**

Additional Buyer terms

Performance of the Service	The service will be delivered in accordance with the supplier's G Cloud service description. OrgVue-service-definition-document.pdf OrgVue_Service Description.pdf

	Link: https://redirect.contractawardservice.crowncommercial.gov.uk/service/426303922263495/version/14
Guarantee	Not Applicable
Warranties, representations	In addition to the incorporated Framework Agreement clause 2.3, the Supplier warrants to the Authority that the Services will be performed by appropriately qualified, experienced, and trained personnel, with due care and diligence and to such high standard of quality as it is reasonable for the Authority to expect in all the circumstances from an experienced and professional service provider and in accordance with all relevant statutory requirements and regulations.
Supplemental requirements in addition to the Call-Off terms	Buyer's right to assign/novate licences for free The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted to: • a Central Government Body; or • to anybody (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer. • If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences. • In the event the Buyer engages a third party service provider to assist with its use of the Services, the Buyer may permit such third party service provider to use the Services solely for the Buyer's benefit and subject at all times to the confidentiality obligations set out in this Call-Off Contract. The Buyer shall remain responsible for the acts and omissions of its third party service providers.

Alternative clauses	Not Applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	Not Applicable
Personal Data and Data Subjects	Annex 1 Schedule 7
Intellectual Property	All information including all Buyer data provided by and/or created on behalf of the Authority shall be owned solely by the Authority. The Intellectual Property in Orgvue will always remain vested in the Supplier.
Social Value	Orgvue's Social Value commitment is included as part of Orgvue's Environmental, Social and Governance (ESG) statement which is available here:  OrgVue-ESG-Statement.pdf https://www.orgvue.com/legal/environmental-social-and-governance-statement/ • Fighting climate change: See "Environment Pillar" in Supplier's ESG statement • Covid-19 recovery: See "Social Pillar" in Supplier's ESG statement • Equal opportunity: See "Social Pillar" in Supplier's ESG statement • Wellbeing: See "Social Pillar" in Supplier's ESG statement

Performance Indicators	Not Applicable

1. Formation of contract

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

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

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

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive of the Framework Agreement.

2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.

Signed on behalf of the Buyer:

Name: ……

Title: ……

Signature: ……

Date: ……

Signed on behalf of the Supplier:

Name: ……

Title: ……

Signature: ……

Date: ……

Buyer Benefits

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

G-Cloud 14 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 36 months

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules 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:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 to 8.6 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 30 (Insurance)
- 31 (Severability)
- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

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

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

2.2.2 a reference to ‘CCS’ or to ‘CCS and/or the Buyer’ will be a reference to ‘the Buyer’

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

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

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

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

3. Supply of services

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

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

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services
4.1.2 apply all due skill, care and diligence in faithfully performing those duties
4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer
4.1.4 respond to any enquiries about the Services as soon as reasonably possible
4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has

completed the Indicative Test, it must download and provide a copy of the PDF with the 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

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

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

9. Insurance

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

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

10. Confidentiality

10.1 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 incorporated Framework Agreement clause 34. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights ("IPR"s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer's or its relevant licensor's Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer's written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;
(b) alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;
(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

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

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

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

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

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

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

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

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

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

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

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

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

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.npsa.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.npsa.gov.uk/sensitive-information-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 Buyer requirements in respect of AI ethical standards.

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

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

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

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

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

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

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

16. Security

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

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

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

16.4 Responsibility for costs will be at the:

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

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

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

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

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

17. Guarantee

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

17.1.1 an executed Guarantee in the form at Schedule 5

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

18. Ending the Call-Off Contract

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

18.2 The Parties agree that the:

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

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

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

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

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

18.4.2 any fraud

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

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

18.5.2 an Insolvency Event of the other Party happens

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

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

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

19. Consequences of suspension, ending and expiry

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

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

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

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

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

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

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

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

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

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

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

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

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

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

19.5.5 work with the Buyer on any ongoing work

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

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

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

20. Notices

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

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

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

21. Exit plan

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

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

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

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

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

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 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 CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

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

21.6.2 there will be no adverse impact on service continuity

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

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

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

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

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

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

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

21.8.4 the testing and assurance strategy for exported Buyer Data

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

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

22. Handover to replacement supplier

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

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

22.1.2 other information reasonably requested by the Buyer

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

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

23. Force majeure

23.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

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

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

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

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

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

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

25.5.2 comply with Buyer requirements for the conduct of personnel

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

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

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

26. Equipment

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

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

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

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

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

28. Environmental requirements

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

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

29. The Employment Regulations (TUPE)

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

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

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement

29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

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

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

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

29.6.1 its failure to comply with the provisions of this clause

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

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

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

30. Additional G-Cloud services

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

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

31. Collaboration

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

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

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

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

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 if it isn't a material change to the Framework Agreement or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request using the template in Schedule 9. This includes any changes in the Supplier's supply chain.

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

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

Orgvue software subscription

- **Service ID**: 426 303 922 263 495
- **Service Description**: https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/426303922263495
- **Service Definition**: https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/92240/426303922263495-service-definition-document-2024-05-02-0807.odt

Orgvue support

- **Service ID**: 453 227 898 661 002
- **Service Description**: https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/453227898661002
- **Service Definition**: https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/92240/453227898661002-service-definition-document-2024-05-02-0807.odt

OD tooling requirements:

- Meet all necessary IG and security requirements
  Orgvue is SaaS, provided on a one to many basis, so it can only be provided one way to all Orgvue customers. That is set out under the Orgvue Security Provisions and Service Level Agreement published on the G-Cloud 14 Digital Marketplace.
- Ability to deal with different data schemas in 2 organisations
- Regular data pulls to ensure up to data is being used.
  Note: To meet this requirement DHSC & NHS England will need to publish data to be refreshed to a single SFTP site. Complete data separation prior to DHSC and NHS England merger, pulling from two SFTP sites, could be achieved through the use of two separate Orgvue tenants, one for DHSC and one for NHS England. The more typical method is for the customer to push data into Orgvue either via CSV file or Orgvue API. A hybrid approach is also possible, for example Orgvue could pull data from one organisation's SFTP site while the other organisation pushes data into Orgvue's secure file store.
- Provide a single view of both organisations today with current state structure & cost analysis
- Quickly identify and address data quality priorities
- Segregate views of data from the two current orgs until they are legally merged, for data protection

Note: Orgvue supports this for regular users of the platform. The Authority “admin” users will have access to all data in the Orgvue tenant they have access to. Complete data separation prior to DHSC and NHS England merger could be achieved through the use of two separate Orgvue tenants, one for DHSC and one for NHS England.

- Capability to provide scenario modelling, to deliver change in a number of stages.
- Rapid production of org charts
- Report on design scenarios as compared to the baseline (headcount, cost)
- Report of structures against set design parameter and identify outliers i.e. spans and layers
- Change tracking and control capability
- Provide data to help with change management, comms, and implementation
- Support placement of staff in to positions in future
- Manage and visualise actuals vs budgets vs forecasts of FTE, cost and headcount over time
- Build capability (method, skills, tooling) for ongoing org change
- System configuration to align to business needs including permissions etc
- Solution must be able to be stood up and operations in a 6-8 week period
- Proven solution with evidence of utilisation in large scale organisational change programmes / mergers
- Upskilling and training of staff to effectively use tooling
- Technical support throughout change programme

The following Services Descriptions are hereby incorporated below. For the term “Customer” and “Buyer” shall be interchangeable.

1. Orgvue Activation,
2. OD configuration & upskill services,
3. Tracking & Monitoring configuration & upskill services.
4. Silver success package

SERVICE DESCRIPTION 1

Orgvue Activation

Context

NHS England and DHSC are undertaking a significant organisational transformation, bringing together approximately 22,000 staff under a unified operating model. The organisations currently use separate HR systems with different data schemas. Historically, organisational design and reporting have been conducted in Excel and PowerPoint, limiting modelling capability, data quality oversight, and stakeholder engagement.

This Orgvue Activation project will establish a secure, configured Orgvue environment to provide a single view of current organisational structures, support ongoing data refresh, and enable future design and modelling activities.

Objectives

The Customer are purchasing Orgvue to support organisation wide modelling activities and need Orgvue Professional Services support to activate the tenant, configure the data refresh process, and enable their central administrators in the ongoing use and maintenance of the tenant.

Requirements

The Customer has entered into the Orgvue Master Services Agreement; as such the Customer requires the as-is model of its in-scope employees to be configured and secured correctly for end-user insight consumption (reporting). The Customer therefore requires:

- Support in configuring Single Sign On (SSO) for user authentication to the Customer Orgvue Environment as recommended best practice;
- Support in configuring any IP Whitelisting requirements on the Customer Orgvue Environment (where the Customer desires this to occur);
- Support in mapping Customer's Source Data into the People, Position and Link Datasets that will most appropriately represent the as-is model of in-scope employees in Orgvue;
- Support in providing a method for Customer Administrators to refresh the Customer's Source Data into the People, Positions and Links Datasets when new Customer Source Data becomes available;
- Acceptance Testing support for Customer Administrator throughout the Activation Project;
- Administrator training for ongoing environment management.

Deliverables

The Deliverables (D01-D06) and associated Acceptance Criteria underpinning these objectives are detailed in the tables contained in 2.4 Deliverables and 2.9 Acceptance (which define the scope of this Service Description).

Ref	Deliverable	Input	Description	Output
D01	Activation Framework	Signed MSA	The Services Team will deploy the Activation Framework to the activated Customer Environment. The Services Team will share the Orgvue Knowledge Base which will introduce key concepts for new users to the Orgvue platform.	Customer Environment available to Customer Administrator with standard dataset containers available. These will include a People, Positions, and Links Dataset (depending on architecture). Depending on Data Ingest approach (Implementation Hub, Customer-Managed API Integration, or 3rd Party Connector Integration) the dataset containers may or may not yet have Customer Source Data included at this point. Customer Administrator will have received relevant Knowledge Base access that can be shared with other members of the Customer team as relevant.
D02	Data Ingest requirements documentation	D01 – Activation Framework (For Implementation Hub approach and Customer-Managed API Integration approach): Sample	Maximum one full time equivalent (FTE) day for remote workshops to: Confirm SSO Requirements (and if required to complete prior to Data Ingest) Confirm IP Whitelisting Requirements (and if required to complete	If SSO or IP Restrictions are required prior to Data Ingest then this will be documented and applied to project plan and dependencies. (For Implementation Hub approach): Customer Source Data

		Customer Source Data (should be accessible during the workshop) (For 3rd Party Connector Approach): access to Customer Source Data Environment should be made available to the Orgvue Services Team	prior to Data Ingest) Review Customer Source Data schema Determine the appropriate Master / Subtenant Architecture for Customer's requirements Map Source Data (and required calculated properties) into the Property Mapping template in the Implementation Hub (or document via alternative approach for Customer-Managed API Integration approach or 3rd Party Connector Approach) Define all data refresh configuration options available in the Implementation Hub (Customer to manage data refresh considerations for Customer-Managed API Integration or 3rd Party Connector Approach)	for People, Positions and Links Dataset mapped in the Implementation Hub, as are data refresh configuration options and these are available to share with Customer Administrator for signoff. (For Customer-Managed API Integration approach or 3rd Party Connector Approach): Property Mapping and data refresh considerations are documented outside of the Implementation Hub and Customer Administrator will coordinate ongoing management of these requirements on the Customer side moving forward as required. The Supplier will work with the Customer to consolidate these outputs into a data flow map, including Customer data sources, data paths, cadences and accesses.
D03	Data Ingest Acceptance Testing	Data Ingest requirements documentation (D02)	Up to one day FTE time to support the Customer in running the Acceptance Testing process. Support will be provided remotely unless specifically agreed by Customer and Orgvue. Acceptance Testing will be supported through the Data Quality Packs templates available in	Any specific issues flagged by the Customer Administrator will be jointly reviewed by the Orgvue Services Team and Customer Administrator. Issues related to Data Ingest configuration will be amended and the Data Ingest process refreshed again to

			the Orgvue platform. The Orgvue Services Team and Customer Administrator will review to verify the data outputs match what is expected based on D02 Data Ingest requirements documentation: Number of nodes in each of People, Position and Links Datasets is correct according to D02. Number of properties in each of People, Position and Links Datasets (including names and data types) is correct according to D02. Data Ingest configuration options correctly reflect D02.	review the new results. Separately, any issues related to Customer Source Data quality will not be deemed as related to the signoff of this deliverable.
D04	Administrator Training and Tenant Management & Handover Session	Property Mapping & Data Ingest Acceptance Testing (D04)	Up to 0.5 FTE day for working sessions with Customer Administrator(s) to review best practices for managing the Customer Environment. Topics to include: Tenant and dataset architecture review & documentation Adding users and managing user permissions Overview of end-to-end Data Ingest process. Overview of the Gizmo expression language in Orgvue	Administrator Training and Tenant Management & Handover Session delivered to Customer Administrator.
D05	Configured Customer Environment	Property Mapping & Data Ingest Acceptance Testing (D03) Administrator	Customer Environment will be configured and secured in accordance with requirements specified in D02 & D03. Completion of Tenant	Customer Administrator has administrator access to the configured Orgvue platform and the Implementation Hub, in

		Training and Tenant Management & Handover Session (D04)	Management & Handover Session (D04).	order to manage the Customer Environment moving forward.
D06	Organisation Analysis	Configured Customer Environment	One 2-hour workshop with executive sponsor to playback organisation analysis, insights, and findings following initial load of Customer data into Orgvue tenant.	As-is organisation analysis covering key organisation metrics (data permitting) including but not limited to: Span of control Organisation layers FTE Cost Headcount Grade compression Contractor analysis

Pre-existing materials

- Orgvue licence agreement (see Service ID 426 303 922 263 495)
- Customer Orgvue environment
- Customer Source Data environment
- Consolidated Customer Source Data from Customer Source Data Environments and agreed process to load into the Orgvue Activation Framework in the Customer Orgvue Environment via Data Ingest

Assumptions

Key assumptions are:

- Customer information technology team have approved Orgvue and are represented in the Customer project team;
- Named Customer Administrator with the authority to agree the backlog of tasks for the Orgvue resource(s) to deliver against;

Dependencies

This project has the following dependencies

- The Orgvue Services Team resource(s) will have administrator access to the

Customer Environment (as required throughout the Activation Project);

- Availability of relevant Customer Source Data from the Customer Source Data Environment to be provided for Data Ingest into the Orgvue Customer Environment;
- Customer Administrator has access to Customer Source Data for required inputs to configure the Activation Framework (via Property Mapping);
- Orgvue Services Team resource(s) will have appropriate access to the Customer Source Data Environment (where a 3rd Party Connector Integration approach is used for Data Ingest) – specific access rights to be aligned between the appropriate Customer team and the Orgvue Services Team to ensure access is sufficient to complete the agreed work;
- Reasonable access to Customer's key stakeholders are provided to the Orgvue Services Team.

Exclusions

The following items are considered out of scope for this project:

- Any custom development of the Orgvue platform (configuration of the Orgvue platform is supported but customization of the Orgvue platform is not in scope for this project);
- Responsibility for the Orgvue Services Team to provide services support for the Customer's Data Ingest process, after D5 (Configured Customer Environment) is accepted.

Acceptance

Ref	Deliverable	Acceptance process	Acceptance criteria	Result of non-acceptance
D01	Activation Framework	Named Customer Administrator(s) is given access to the newly configured Customer Environment. Named Customer Administrator(s) will have the Orgvue Knowledge Base shared with them by the Orgvue Services Team.	Named Customer Administrator can access the newly configured Customer Environment. No data will be available at this point. SSO and IP Whitelisting will not be required at this stage. The Orgvue Administrator(s) will	N/A

			have received links to the Orgvue Knowledge Base	
D02	Data Ingest requirements documentation	(For Implementation Hub approach): Customer Administrator and Services Team representative use the Implementation Hub to document all Property Mapping and data refresh requirements. The Implementation Hub will use a set of stage-gates to gather all requirements to completion live within the workshop(s). Customer Administrator and Services Team member will sign off that requirements are complete using the Implementation Hub (or another agreed-upon written format) before D03 or D04 can begin. (For Customer-Managed API Integration or 3rd Party Connector Integration approach): The Orgvue Services team and Customer Administrator will agree upon a property mapping and data refresh requirements template that will then inform the Customer Administrator's ongoing management process moving forward. Requirements will be signed off before D03 or D04 can begin.	(For Implementation Hub approach): The Customer Administrator will sign off in writing that the Implementation Hub should be used to perform an initial Data Ingest and that the existing configuration is correct and signed off for that purpose. (For Customer-Managed API Integration or 3rd Party Connector Integration approach): The Customer Administrator will confirm in writing (on an agreed template format) that the Property Mapping and data refresh configuration requirements are correct so that the team can begin relevant build and testing phases. In any approach, work on D03 and D04 cannot begin until D02 is signed off as complete.	Until the Customer Administrator has provided written sign-off of Data Ingest requirements documentation, the Activation Project will not proceed to D03 or D04. The Activation Project will be paused until sign-off on D02 requirements is achieved (this may potentially impact overall project timelines).
D03	Data Ingest Acceptance Testing	The Acceptance Testing will be performed by Customer in the Customer Environment, and	The Customer Administrator will sign off in writing that all Data Ingest	The Customer Administrator must explicitly indicate (using the Data

	following the agreed Acceptance Test scripts template (using the Orgvue Data Quality Packs). The Customer Administrator must confirm in writing to the Services Team that the Acceptance Test has been met.	Acceptance Testing has been achieved (i.e. no configuration issue is raised) before D05 can begin. The Customer Administrator must confirm in writing to the Activation Team that the Acceptance Test has been met. Note: Issues related to the quality or accuracy of Customer's Source Data do not constitute a configuration issue.	Quality Packs provided by the Orgvue Services Team) any configuration issues that have occurred as part of the Data Ingest Refresh Acceptance Testing process. Orgvue will work to correct all confirmed gaps between Data Ingest requirements and the outputs of the Data Quality Packs and provide fixes batched together where practical. Orgvue will be responsible for addressing any and all configuration issues (according to the Data Quality Packs review) required to complete D03, without any extra time or cost implications to Customer. Until the Customer Administrator has provided written sign-off of Data Ingest Acceptance Testing, the Activation Project will not proceed to D04. The Activation Project will be paused until sign-off on D03 is achieved (this may potentially impact overall project timelines).

D04	Administrator Training and Tenant Management & Handover Session	Training delivered at the agreed date, time and place.	Timesheet reports can be provided on request.	N/A
D05	Configured Customer Environment	When D03 & D04 are accepted, D8 will be deemed accepted.	Signed-off Deliverables D0 & D04.	N/A
D06	Organisation Analysis	Analysis delivered at the agreed date, time and place.	Timesheet reports can be provided on request.	N/A

Service Description 1 Appendix

Item	Description
3rd Party Connector Integration	For Customers who wish to perform Data Ingest operations to the Orgvue platform through an external integration (i.e. not the Implementation Hub) however also do not wish to develop a Customer-Managed API Integration approach, the option for a 3rd Party Connector Integration can be leveraged (depending on Customer Source Data Environment). Technical details and approaches must be validated prior to confirming this approach; where appropriate the Orgvue Services Team can leverage a 3rd Party Connector Integration approach (which may have technical and commercial considerations in addition to the scope of this Service Description). Ongoing management / maintenance of the Data Ingest process using a 3rd Party Connector Integration will be outlined in an additional Service Description specific to the Customer's technical landscape.
ABAC	An acronym that stands for Attribute-Based-Access-Control, and refers to the ability to configure Orgvue user access rights for a particular data element (node and property combination). In a practical sense, ABAC refers to row-level access rights within the Orgvue platform.
Activation Framework	A set of configuration and Orgvue dataset schemas that are deployed to the Customer Environment at the start of the Activation Project. The initial deployment of the Activation Framework by the Services Team satisfies D1 in this Service Description. Depending on the Data Ingest approach (Implementation Hub, APIs, or Connectors) the datasets may or may not yet have data when the Activation Framework is deployed (this is methodology dependent).
Activation Project	The full scope of activities contained in this Service Description. The goal of this project is to deploy and configure the Activation Framework to the

	Customer Environment, and provide appropriate training and documentation for the Customer Administrator in order to manage the Customer Environment on an ongoing basis after the project is complete.
Acceptance Testing	The process of testing that both Orgvue and Customer perform to ensure that system configuration correctly reflects requirement documents during the Activation Project. Where Acceptance Testing is required for specific deliverables in the Activation Project, Orgvue will provide a standard template (i.e. document or Orgvue pack) as a mechanism to evaluate all required test cases.
Administrator Training	A training session targeted at Customer Administrators that cover the key activities in the Activation Project to allow the Customer Administrator to maintain the Orgvue Environment on an ongoing basis.
Baseline Plan	A step in building a workforce plan that identifies the time horizon, base dataset and properties to be used in establishing the foundation of a plan.
CCN	Change Control Notice
Customer Administrator	A nominated individual in the Customer's organisation, who acts as a central point of contact and sign-off authority for all activities in the Activation Project. The Services Team will liaise directly with the Customer Administrator for the sign-off of project deliverables and will furthermore ensure that the Customer Administrator is equipped (through training and configuration documentation) to act as an administrator of the Customer Environment.
Customer Environment	The Tenant (or set of Tenants in a Master/Subtenant Architecture) that collectively make up a Customer's use of Orgvue as a platform. The entire Customer Environment is covered under a single commercial agreement.
Customer-Managed API Integration	For Customers who wish to perform Data Ingest and / or Export operations to the Orgvue platform via a Customer-Managed API Integration approach and who do not require Orgvue to lead on that work, any development and configuration (Property Mapping and any data validation/refresh considerations) will be required to be managed by the Customer (external to the Orgvue platform). The Orgvue Services Team will share relevant documentation related to Orgvue's API capability that can be leveraged by the Customer's relevant technical teams as part of the Customer-Managed API Integration. The Customer will need to advise the Orgvue Services Team as to resources, capability and anticipated timelines for any internal governance steps required to inform project planning for the Activation Project. Ongoing management for the Customer-Managed API Integration approach will be the responsibility of the Customer.
Customer Source Data Environment	For a Customer who wishes to utilize a 3rd Party Connector Integration approach for Data Ingest and / or Export, members of the Orgvue Services Team will require appropriate access to the platform where the Customer Source Data resides in order to configure the 3rd Party Connector (the Customer will ensure that appropriate access and permissions to that

	platform are available for the work to proceed).
Data Quality Packs	Specific reporting objects in the Orgvue platform that are available as templates that can be applied to any Orgvue dataset. These packs are specifically used in the Data Ingest Acceptance Testing process (please see relevant deliverable).
Defined Training	The full scope of training that will be provided to the Customer as part of the Activation Project. This consists of the Orgvue Knowledge Base, and training for Customer administrators.
Data Ingest and / or Export	The full scope of configuration options available to the Customer by the Orgvue team which may consists of the following key approaches: • Ad-hoc (i.e. manual) upload of Customer Source Data via Orgvue Settings. This approach is helpful for quick initial Data Ingest but is not automated in terms of subsequent Data Ingests. This approach can often be used as a starting point for Customer-Managed API Integrations or 3rd Party Connector Integration approaches. Ad-hoc (i.e. manual) export of Orgvue data is also possible to a ,CSV or .TSV file. The data to be exported can be controlled by the user, subject to the user having the appropriate permissions. • Implementation Hub (Orgvue platform-managed for Data Ingest) : The Orgvue Services team will gather requirements with the Customer Administrator to document Property Mapping and other validation steps related to Data Ingest. This approach requires .csv (or .csv.pgp) file inputs to the process which should be supplied by the Customer Administrator. • Customer-Managed API Integration approach for data ingest and / or export: The Orgvue Services team will share relevant documentation on Orgvue's API's that can be called by a Customer-Managed API Integration (which must be managed entirely by the Customer). In this approach the Property Mapping and other validation steps will be documented between the Orgvue Services Team and the Customer Administrator. Ongoing management of this integration approach would be the responsibility of the Customer. 3rd Party Connector Integration approach for data ingest and / or export: The Orgvue Services team will run a workshop with the Customer Administrator in order to confirm Property Mapping that should be leveraged by the 3rd Party Connector Integration. The Orgvue Services team will then configure the 3rd Party Connector Integration according to the Property Mapping (and other validation items to be agreed, possibly including export process) and will advise when Acceptance Testing can begin. In this approach, the Customer will be required to grant appropriate access/permissions to the Customer Source Data Environment as needed to complete this work. This is covered by a separate Service Description.
Implementation Hub	The Implementation Hub is an interface of the Orgvue platform that manages the Data Ingest process (for Customers who wish to use this Data

	Ingest methodology). This interface expects to perform Data Ingest operations using Customer Source Data (expected as either .csv or .csv.pgp inputs). Customer Administrators will receive training on how to manage the Implementation Hub as a method of managing the Data Ingest process even after the completion of the Activation Project. The Implementation Hub offers automation through schedules and connections to a customer-hosted SFTP server (if desired) by way of SSH key authentication.
IP Whitelisting Requirements	IP Whitelisting allows users to access Orgvue from only a select number of IP addresses. If a user attempts to access Orgvue from outside the whitelisted IP address then the user will not be able to access Orgvue until they return to the whitelisted IP/Subnet. The Services Team will be able to work with the Customer Administrator during the Activation Project in order to enable IP Whitelisting for the Customer Environment, and can provide any further technical details on how to proceed at that time.
Knowledge Base	An online reference knowledgebase for the Orgvue platform, covering a range of different topics relevant to Customers who use the Orgvue platform.
Links Dataset	The Orgvue dataset that relates nodes in the People Dataset to nodes in the Positions Dataset in a many-to-many relationship. The Links Dataset allows for robust modelling of vacancies and position sharing within the Customer organisation through Orgvue.
Master / Subtenant Architecture	A Master/Subtenant Architecture refers to the ability for Orgvue to relate multiple Tenants in a parent-child structure, which allows configuration to be stored centrally and cascaded throughout a Customer's Environment. Multiple tenants arranged in this structure may be recommended for larger-scale organisations, especially if user access rights are logically partitioned along functional or geographic lines (for example). Some organisations may have a simplified set of business and technical requirements, in which case the Master/Subtenant Architecture will reduce to require only a single Tenant for the Customer Environment. The Orgvue Services Team will evaluate the extent to which any such Master/Subtenant Architecture is required (or not) for the Customer's requirements.
People Dataset	The Orgvue dataset that serves as the master version of all people (i.e. employee) data, as provided through the Customer's Source Data.
Positions Dataset	The Orgvue dataset that serves as the master version of all position data for the Customer organisation, as provided through the Customer's Source Data.
Property Mapping	The process of relating each field in the Customer's Source Data to properties in the People, Position and Links Datasets in Orgvue. For the Implementation Hub approach: Property Mapping is managed directly in the Implementation Hub interface. Property Mapping may also be re-configured by the Customer Administrator after the Activation Project is complete, through the use of the Implementation Hub. For the Customer-Managed API Integration approach: Property Mapping is

	agreed between the Orgvue Services Team and Customer Administrator in an agreed format (such as excel or other). Relevant configuration based on this agreed Property Mapping is managed by the Customer in the Customer-Managed API Integration. For the 3rd Party Connector Integration approach: Property Mapping is agreed between the Orgvue Servies Team and Customer Administrator in an agreed format (such as Excel or other). Relevant configuration based on this agreed Property Mapping is managed by the 3rd Party Connector Integration.
RBAC	An acronym that stands for 'Row-Based-Access-Control', and refers to the ability to configure Orgvue user access rights to a set of datasets (or properties within a given dataset). In a practical sense, RBAC refers to dataset-level (or property-level) access rights within the Orgvue platform.
Services Project Lead	The most senior resource on the Services Team who acts as the key point of escalation during the Activation Project. The Activation Project Lead will be identified as part of the Services Team on or before the commencement of the Activation Project.
Services Team	Orgvue resources assigned to work directly with the Customer Administrator throughout the Project. Named resources will be assigned at or before the commencement of the Project.
Settings	An interface of the Orgvue platform that is used to manage metadata of various objects in the Customer Environment (primarily datasets and user access). The Settings interface is the area of a platform where a Customer can perform an ad-hoc (manual) data upload.
Source Data	The scope of organisational information the Customer will be loading into Orgvue as part of the Activation Project. For the Implementation Hub approach: This information is contained in one (or multiple) .csv files (and in many cases is an extract of an HRIS system). This information typically contains field (columns) related to either employee or position attributes (such as name, gender, department, salary, employee ID, position ID), and each record (row) typically relates to a single employee (or position) within the organisation. These files may reside within an SFTP location, or can be uploaded to the Orgvue platform's files endpoint as the starting point for the Data Ingest process. PGP encryption of these .csv files is supported (and the expected format would then be .csv.pgp). For the Customer-Managed API Integration approach: This information is contained in one (or multiple) .csv files or JSON files (and in many cases is an extract of an HRIS system). This information typically contains field (columns) related to either employee or position attributes (such as name, gender, department, salary, employee ID, position ID), and each record (row) typically relates to a single employee (or position) within the organisation. The generation, relevant transformation steps (if any) and push of this data to the Orgvue platform are required to be entirely managed by the Customer in the Customer-Managed API Integration Data Ingest

	process. For the 3rd Party Connector Integration approach: This information is contained in the Customer's HRIS (Customer Source Data Environment) and pulled via the 3rd Party Connector Integration into the Orgvue platform (typically as a JSON object). This information typically contains field (columns) related to either employee or position attributes (such as name, gender, department, salary, employee ID, position ID), and each record (row) typically relates to a single employee (or position) within the organisation. The generation, relevant transformation steps (if any) and push of this data to the Orgvue platform are entirely managed by the 3rd Party Connector Integration Data Ingest process.
SSO Requirements	Orgvue provides Single-Sign-On (SSO) using SAML 2.0 for user authentication to access the Orgvue Customer Environment. In order to enable SSO for the Customer Environment, the Customer must provide federated metadata, in the form of an XMLS file, containing: Crypto certification (both Sha1 and Sha256 are supported) The URL to the Customer's IdP The Services Team will be able to work with the Customer Administrator during the Activation Project in order to enable SSO for the Customer Environment, and can provide any further technical details on how to proceed at that time. Orgvue recommends configuring SSO for user authentication as best practice (however also supports local password management by default).
Tracking & Monitoring Dataset(s)	Tracking & Monitoring solution dataset(s) that are deployed to the Customer Environment at the start of the project. These will include a timeseries and/or detailed changes ("JML") dataset, which will be determined based on reporting requirements defined during workshop. The timeseries dataset stores period-by-period cost and headcount data aggregated by pre-defined dimensions, while the detailed changes or "JML" (acronym for "Joiners, Movers, and Leavers") dataset stores position or person-level changes between two periods.
Tracking & Monitoring Standard Reports	The standard Orgvue pack(s) that will be built on top of the Tracking & Monitoring dataset(s) that serve to visualize and report on the data.
Tenant Management & Handover Session	During the Activation Project, the set of training that the Services Team will provide to the Customer Administrator in order to allow the Customer Administrator to manage the Customer Environment on an ongoing basis (overview and handover of: dataset architecture, Data Ingest, and user access management).
User Permissions	The collective set of access rights that exist between any in-scope Orgvue users and in-scope datasets within the Customer Environment. User Permissions are comprised of a combination of ABAC and RBAC logic and determine the level of access (invisible, visible, update, edit) a user has to a

particular data element within the Orgvue platform.

SERVICE DESCRIPTION 2

Org Modelling Configuration

Context

NHS England and DHSC are undertaking a significant organisational transformation, bringing together approximately 22,000 staff under a unified operating model. The organisations currently use separate HR systems with different data schemas. Historically, organisational design and reporting have been conducted in Excel and PowerPoint, limiting modelling capability, data quality oversight, and stakeholder engagement.

As part of the integration activities, the Customer requires the configuration of custom organisation modelling workflow within their Orgvue platform. These workflows are critical to effectively managing the transformation and optimising the combined workforce structure. The organisation modelling capability will enable the Customer to create and evaluate a future state organisation structure and optimise headcount allocation.

Objectives

- Load position and people data from both organisations
- Configure a custom Org Modelling workflow to support the design of a single future state organisation
- Create M&A focussed packs to show progress, outcomes and impacts
- Configure access to ensure users see only the relevant slices of data

Requirements

The Orgvue Professional Services team will support the Customer with the following activities:

- Create a solution in Orgvue to support the modelling of a future state organization and understand the impact of design decisions. The solution should enable the Customer to:
    - Review the baseline organization, define scope and decide where to investigate and model
    - Model one or multiple future scenarios by capturing position level changes
    - Capture critical information for the model including effective date and reason if applicable
    - Review the new, closed and changed positions to support the implementation of the model

    - Resolve design errors related to hierarchy, missing data and out of scope changes
    - Compare the model against baseline to understand impact on size, cost and other metrics
    - Understand the impact of modelled changes on size and cost over time
- Configure user access framework to enable the Customer to view or capture the right decisions for their segment of the organisation
- Provide training to enable the Customer to use Orgvue for Org Modelling work effectively
- Provide Customer with access to Org Modelling User and Administrator Training documentation

Deliverables

Ref	Deliverable	Input	Description	Output
D1	Org Modelling Requirements	Customer source data Customer stakeholders with knowledge of source data, org modelling process and user permission requirements	On-site or remote workshop(s) to: • Review source data from HRIS and define required data, data flows and calculations for the org modelling process • Define reporting needs and user workflows to facilitate the org modelling and impact analysis process • Define user groups and their access levels to hide, view or update certain data fields (i.e. properties) or segments of the organisation (i.e. workstreams)	Requirements for data fields, calculations, reports, workflows, user groups and access levels documented and signed off by the Customer This document will act as the Acceptance Test script for all parties
D2	Org Modelling Configuration	Customer source data D1	Custom workflows and reports aligned to the Org Modelling Requirements to enable: • Modelling of the current organisation into a new future organisation • Visualizing impact on size, cost and structure between the current and future organisation	Configured Org Modelling Template available to Customer in Orgvue tenant including source data and tailored reports and workflows
D3	Org Modelling Acceptance	D1 & D2	Acceptance Testing template and support available for Customer to	Signed off documentation

	Testing		verify the Org Modelling Solution appears in Orgvue tenant with correct outputs, functionality and user permissions according to Org Modelling Requirements	indicating the Org Modelling Solution is functioning as defined in D1
D4	Org Modelling User Training	D2 & D3	Two-hour trainer-led session for up to 20 attendees to build Customer's capability to navigate the Org Modelling Solution including: • Org Modelling process • Org Modelling workflows and reports in Orgvue • Orgvue exercises	Org Modelling User Training delivered to Customer attendees Org Modelling User Training documentation shared with the Customer
D5	Org Modelling Administrator Training	D2, D3 & D4	Two-hour training-led session for up to 8 Customer Administrators to build capability to manage the Org Modelling Solution including: • Detailed architecture overview • Add users with correct permission • Manage properties and lookups • Create backups and update data	Org Modelling Admin Training delivered to Customer Administrator Org Modelling Admin Training documentation shared with the Customer

Pre-existing materials

- Orgvue licence agreement (see Service ID 426 303 922 263 495)
- Customer Orgvue tenant
- Customer source data

Assumptions

Key assumptions are:

- Baseline data (as-is) is static and does not need to be refreshed during Org Modelling project
- Customer source data is accurate and does not require any cleaning by the Supplier
- Number of positions in scope for the Org Modelling solution is below 40,000

Dependencies

This project has the following dependencies:

- Orgvue resources will have administrator access to the Customer tenant
- Customer resources attending workshops and reviewing requirements documents have the authority to sign off on their contents on behalf of Customer
- Reasonable access to key Customer stakeholders
- Customer resources have access to source data

Exclusions

The following items are considered out of scope for this project:

- Any custom development of the Orgvue core product
- Responsibility for any on-going data-loading into Customer tenant after project acceptance
- Updates to design in Orgvue based on offline design documents (e.g., Excel, PowerPoint)
- Process for integration or comparison between multiple scenarios
- Training to setup new org modelling solutions for additional transformations
- Updates to any logic after requirements have been approved and the solution has been accepted
- Configuration of talent selection workflow
- Facilitation of org modelling activity in the platform

Payment milestones

Orgvue has estimated the time and resources to produce the deliverables to the required level of detail and quality, and the estimated cost is detailed below. Billing will occur on completion of project phases as listed below.

Except to the extent the Professional Services and/or Deliverables are delayed because of Department for Health and Social Care failure to perform its obligations under this Service Description, Orgvue will be able to complete this work. However, if there is such Department for Health and Social Care caused delay in the timeline, Orgvue will invoice Department for Health and Social Care on a time & materials basis by the end of the month for the work completed in month.

Notwithstanding any other provision, Orgvue will keep the Customer updated by email without delay if it considers that its fees under this Service Description For Professional Services are likely to exceed [redacted], and will (for the avoidance of doubt) only charge in respect of days worked by the persons/roles outlined herein.

Phase	Milestone	Deliverables	Cost
1	Project Initiation	Project plan, kick-off meeting	[redacted]
2	Org Modelling Requirements	Approved requirements document for Org Modelling Workflow	[redacted]
3	Org Modelling Configuration	Completed testing for Org Modelling workflow, issue resolution	[redacted]
4	Org Modelling Testing	Completed testing for Org Modelling workflow, issue resolution	[redacted]
5	Org Modelling Training	Completed user and admin training for Org Modelling Workflow	[redacted]
6	Technical Document Handover	Final technical documentation, project handover	[redacted]
Total			[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted] individual in the Customer's organisation, who acts as a central point of contact and sign-off authority for all activities in the project. The Orgvue Professional Services team will liaise directly with the Customer Administrator for the sign-off of project deliverables and will furthermore ensure that the Customer Administrator is equipped (through training and configuration

	documentation) to act as an administrator of the Orgvue workflow.
Professional Services	The Orgvue resources assigned to work directly with the Customer Administrator throughout the project. Named resources will be assigned at or before the commencement of the project.
Org Modelling	Org Modelling is the process of adding, removing, and changing positions that exist within an organisation to create a future (to-be) model better aligned to the organisation's goals.
Org Modelling Solution	A set of properties, calculations, dataset schemas, and Orgvue packs that are built in the Customer Environment to support the Org Modelling Process and enable the following: • Visualize as-is organisation and as-is data • Capture to-be data and track new, closed & changed positions • Capture a change reason and track changed properties • Calculate as-is and to-be team size (headcount) and cost using hierarchy • Calculate average to-be cost using rate card based on max 5 dimensions • Calculate span of control & customized span of control group • Calculate delta between as-is and to-be for headcount, cost, and other metrics • Capture scope of design work and flag changes made to out of scope positions • Flag design errors related to hierarchy, missing data & wrong change reason • Capture action date or wave and visualize designed FTE and cost changes in time
Org Modelling Source Data	The scope of Org Modelling data the Customer has in and / or will be loading into Orgvue as part of the Org Modelling project. The data should come from the Customer's HRIS and can be uploaded via the Orgvue data refresh process if Activation has taken place. If no Activation has taken place or additional properties are required, the data can be manually loaded via the Orgvue settings application.
Org Modelling Dataset	The Orgvue dataset that serves as the master version of the to-be organisation structure for the Customer organisation. This dataset contains critical as-is properties from the Source Data and to-be properties actioned and modifiable for design. It also contains standard properties and calculations to support the Org Modelling process (e.g., action).
Org Modelling Tracking Dataset	The Orgvue dataset that enables the visualization of the changing size and cost of the organisation over time (data-based tracking). This dataset imports the design data from the Org Modelling Dataset to enable real-time tracking. This dataset contains properties configured in the Property Mapping stage to enable this functionality.

Org Modelling Actions	A calculated property showing the action of each position used to track the progress of the Org Modelling project. Inputs for the calculations are critical to-be properties, scope, and flags for removal & reviewed. • To Be Reviewed: Position has not been changed or reviewed. • Unchanged Position: Position has been reviewed but no critical to-be properties were changed. • Changed Position: One or multiple critical to-be properties have been changed. To-be cost for this position will be an average from the rate card (if applicable). A Change Reason can be captured via a dropdown to capture additional rationale. • Closed Position: Position has been flagged for removal and will no longer exist in to-be organisation. To-be headcount & cost will be set to zero. • New Position: Position is newly created in Orgvue and does not exist in as-is. As-is headcount & cost will be zero, to-be headcount will be 1, and to-be cost will be an average from the rate card (if applicable). • Out of Scope: Position is in the dataset to preserve the org hierarchy or overall numbers but is out of scope for the Org Modelling process. Any changes made to these positions will be flagged in the Validation Flags.
Org Modelling Validation Flags	A suite of calculated validation flags typically included in the Org Modelling Solution: • Higher-level manager is closed but at least one active position is still reporting to it • Change Action and Change Reason property are not aligned. • At least one of the critical to-be fields is not filled in. • An out-of-scope position has had changes of some kind applied.
Org Modelling User Groups	The typical list of Orgvue user groups that engage with the Org Modelling process in Orgvue: • Admins: Administrators that can edit all datasets, packs, and properties in the Customer Environment. • Updaters: Users that execute the Org Modelling Process in Orgvue can update all to-be properties and other relevant modelling properties. As-is properties will be read-only to keep the as-is the same as the Source Data. • Viewers: Users that the track progress and impact of the Org Modelling Process can only view properties in Orgvue, not update.

SERVICE DESCRIPTION 3

Tracking & Monitoring Configuration

Context

NHS England and DHSC are undertaking a significant organisational transformation, bringing together approximately 22,000 staff under a unified operating model. The organisations currently use separate HR systems with different data schemas. Historically, organisational design and reporting have been conducted in Excel and PowerPoint, limiting modelling capability, data quality oversight, and stakeholder engagement.

As part of the integration activities, the Customer requires the configuration of a tracking and monitoring workflow within their Orgvue platform. The tracking and monitoring capability will enable the Customer to measure progress against targets, identify issues early, and optimise decision-making throughout the transformation process.

Objectives

The Customer are purchasing Orgvue to support organisation wide modelling activities and need Orgvue Professional Services support to configure ongoing tracking and monitoring of key performance indicators and metrics over time and enable their central administrators in the ongoing use and maintenance of the tracking and monitoring configuration.

Requirements

The Orgvue Professional Services team will support the Customer with the following activities:

- Create a solution in Orgvue to support the tracking of the actual organisation against the planned organisation over time at an aggregate level. The solution should enable the Customer to:
    - Understand actual size and cost over time based on monthly extracts from the HRIS
    - Understand planned size and cost over time based on the future state model in Orgvue and planned actions and effective dates
    - Compare actuals against plan over time to understand progress and adherence to the planned model at an aggregate level
    - Understand target size and cost over time and compare against actuals and plan at an aggregate level (if available)
    - Drill into different part of the organization to understand progress and deviation by key reporting dimensions (e.g., function, location, department)

- Create a solution in Orgvue to support the tracking of the actual organisation against the planned organisation at a position level. The solution should enable the Customer to:
    - Identify positions that have been added, removed, or changed to the current organisation based on monthly extracts from the HRIS
    - Compare current state changes against the planned actions of the future state model in Orgvue to understand what part of the model is implemented, delayed and still pending
    - Identify unplanned position changes, such as unauthorized hiring, causing deviation from your future state model that may be driving unexpected cost or risk
- Align with the existing security framework to enable the Customer to view the tracking reports for their segment of the organisation
- Provide training to enable the Customer to use Orgvue for the tracking reports effectively
- Provide Customer with access to training documentation

Deliverables

Ref	Deliverable	Input	Description	Output
D1	Advanced Tracking Requirements	Customer Source Data Customer Target and/or Plan data to track against	On-site or remote workshop(s) to: • Review source data from HRIS, plan and targets, and define required data and data flows • Define reporting needs including key KPI's and dimensional fields, reporting cadence and period • Confirm alignment with the existing user groups and security framework to control access	Requirements for KPI's, dimensional fields, source data, reporting cadence, and reporting period documented and signed off by the Customer This document will act as the Acceptance Test script for all parties
D2	Aggregate Tracking Solution	D1	Custom reports aligned to the Advanced Tracking Requirements to enable: • Comparison of actuals against plan and, if available, targets over time to monitor progress and adherence at an aggregate	Aggregate Tracking reports available to Customer in Orgvue tenant including source data, to-be design and targets

			level • Drill-down capability to review progress and deviations by key reporting dimensions	
D3	Position Level Tracking Solution	D1	Custom reports aligned to the Advanced Tracking Requirements to enable: • Comparison of changes against the planned actions in the future state model to track progress and delays at the position level • Identification of unplanned changes that cause deviation from the model	Position Level Tracking reports available to Customer in Orgvue tenant including source data and to-be design
D4	Advanced Tracking Acceptance Testing	D1, D2 & D3	Acceptance Testing template and support available for Customer to verify the Advanced Tracking Solution appears in Orgvue tenant with correct outputs, functionality and permissions according to Advanced Tracking Requirements	Signed off documentation indicating the Advanced Tracking Solution is functioning as defined in D1
D5	Advanced Tracking Training	D2, D3 & D4	Two hour trainer-led session for up to 20 attendees to build Customer's capability to navigate the Advanced Tracking Solution including: • Monthly refresh process • Navigating reports in Orgvue	Advanced Tracking Training delivered to Customer attendees Documentation shared with Customer Administrator

Pre-existing materials

- Orgvue licence agreement (see Service ID 426 303 922 263 495)
- Customer Orgvue tenant
- Customer source data
- Consolidated HRIS data from the Customer's source system, loaded into Orgvue via an agreed Data Ingest process
- Plan and/or target data

Assumptions

Key assumptions are:

- Customer source data is accurate and does not require any cleaning by the Orgvue team
- The Orgvue org modelling solution will be the source of the plan data
- Target data must be provided in a flat-file format (e.g., .csv or .xlsx), with consistent dimensional alignment (e.g., Function, Grade, Department) and time-based breakdown (e.g., monthly totals by cost centre) that matches the Orgvue data model. Data mapping or transformation is not included in this scope.
- The ability to detect changes at the position level (e.g., Joiners, Movers, Leavers) is dependent on the consistent availability of position identifiers and timestamps in the source HRIS data.
- Named Customer administrator or a designated resource will be responsible for the advanced tracking data refresh process

Dependencies

This project has the following dependencies:

- Orgvue resources will have administrator access to the Customer tenant
- Customer resources attending workshops and reviewing requirements documents have the authority to sign off on their contents on behalf of Customer
- Availability of relevant Customer source data from the Customer source data environment to be provided for data ingest into the Orgvue Customer environment
- Reasonable access to key Customer stakeholders
- Customer resources have access to source data

Exclusions

The following items are considered out of scope for this project:

- Configuration or inclusion of metrics that cannot be directly mapped at both the position-level and the aggregate level within the Tracking & Monitoring solution (e.g., metrics that cannot be calculated consistently based on position-level activity).
- Non-standard or event-based costs that do not follow a consistent time-based aggregation model, such as:
    - Prorated costs (e.g., costs calculated based on fraction of time worked rather than presence in period),
    - Severance costs,
    - Recruitment costs,
    - One-time or irregular adjustments.
- Metrics not aligned with Orgvue's standard tracking logic, where a position's values

are only counted when active in a given period (e.g., fully loaded cost, FTE, headcount, base salary).

Service Description 3 Appendix

Item	Description
Acceptance Testing	The process of testing that both Orgvue and Customer perform to ensure that system configuration correctly reflects requirement documents during the project. Where Acceptance Testing is required for specific deliverables in the project, Orgvue will provide a standard template (i.e. document) as a mechanism to evaluate all required test cases.
Customer Administrator	A nominated individual in the Customer's organisation, who acts as a central point of contact and sign-off authority for all activities in the project. The Orgvue Professional Services team will liaise directly with the Customer Administrator for the sign-off of project deliverables and will furthermore ensure that the Customer Administrator is equipped (through training and configuration documentation) to act as an administrator of the Orgvue workflow.
Professional Services	The Orgvue resources assigned to work directly with the Customer Administrator throughout the project. Named resources will be assigned at or before the commencement of the project.
Actuals	The recorded, real-time data representing the organization's current state (e.g., headcount, cost, role, department) as captured in HRIS or other source systems during each reporting period
Plan	The projected view of the future state organization, often built using Orgvue's Org Modelling solution. It reflects the intended structure, roles, and workforce size/cost for a future time period.
Target	Benchmark or goal-oriented data set that the customer uses to compare performance. This may originate outside Orgvue and is typically static. Target data can also be a budget our output from a strategic workforce planning exercise.
Joiners, Movers, and Leavers (JML)	A classification method used to assess workforce changes over time: • Joiner: A position added to the Actuals Data since the last reporting period. • Mover: A change in a critical property, which are identified during the requirements gathering • Leaver: A position missing from the most recent Actuals Data since

	the last reporting period.
Aggregate-Level Tracking	Summarizes organizational performance (e.g., headcount, cost) at a high level by comparing Actuals vs. Plan or Target across key dimensions like Function or Department.
Position-Level Tracking	Tracks individual position level changes between Actuals and the planned future state, highlighting specific positions that were added, removed, or changed, planned or unplanned.
Time Horizon	The time period over which tracking or reporting will occur (e.g., monthly, quarterly).
Key Performance Indicator (KPI)	A measurable value that demonstrates how effectively the organization is achieving key goals. Common KPIs include headcount, Cost, Span of control, etc.
Dimensional Fields	Categorical attributes used to slice or filter data in reports (e.g., Function, Geography, Business Unit). These dimensions allow tracking and comparison across organizational segments.
Customer Source Data Environment	The system or location where the Customer's HRIS or workforce data is stored, typically used as the source for Orgvue data ingest.
Consolidated HRIS Data	A unified extract of employee and position data (e.g., from one or more HRIS platforms) formatted to support Orgvue configuration and analysis.
Orgvue Activation Framework	A standardized configuration deployed in the Orgvue environment that includes pre-defined datasets, properties, and structure to enable rapid onboarding and analysis.
Data Ingest	The process of importing customer source data into Orgvue using either the Implementation Hub, API, or manual upload, based on an agreed approach and property mapping.

SERVICE DESCRIPTION 4

Silver Success Package

Context

NHS England and DHSC are undertaking a significant organisational transformation, bringing together approximately 22,000 staff under a unified operating model. The organisations currently use separate HR systems with different data schemas. Historically, organisational design and reporting have been conducted in Excel and PowerPoint, limiting modelling capability, data quality oversight, and stakeholder engagement.

Objectives

The Customer are purchasing Orgvue to support organisation wide modelling activities and need Orgvue Professional Services resources to support ongoing administration, training, and content creation activities in the tenant.

Requirements

The Customer requires up to 8 hours per month of support, from Orgvue resource(s) with the requisite skills, to deliver core administration and centre of excellence activities. These may include but are not limited to:

Administration

- Management of users and user groups
- Solution updates and dataset configurations
- Management and audit of tenant content
- Making updates to improve the performance of the tenant or specific datasets
- Managing the data process

Training

- Training end users on configured Orgvue Solutions
- Delivering Fundamentals training
- Delivering Admin training

Content creation

- Accelerating existing initiatives
- Building analysis packs
- Creation of additional custom calculations
- Tailoring of existing solutions

Deliverables

Ref	Deliverable	Input	Description	Output
D01	Workshops	Activated Customer Orgvue environment Customer Orgvue Admin	Up to four (4) structured two (2)-hour remote workshops per month to support activities agreed with the Customer	Access to resource with the requisite skills and knowledge

Pre-existing materials

- Orgvue licence agreement (see Service ID 426 303 922 263 495)
- Customer Orgvue tenant
- Customer Orgvue Activation documentation

Dependencies

This engagement has the following dependencies:

Orgvue resource(s) will have administrator access to the Customer tenant

Named Customer Product Owner with the authority to agree the backlog of tasks for the Orgvue resource(s) to deliver against.

Exclusions

The following items are considered out of scope for this engagement:

Deployment of Orgvue solutions, not already configured by the Orgvue Expert Services team

Programme management activities related to any ongoing initiatives within the Orgvue platform

Execution or facilitation of Orgvue workshops and/or sessions related to ongoing initiatives within the Orgvue platform

Rollover of unused hours from one month to the next.

Acceptance

Ref	Deliverable	Acceptance process	Acceptance criteria	Result of non-acceptance
D01	Resources	Resources with requisite skills are provided at the agreed date, time and place.	Timesheet reports can be provided on request.	

Schedule 2: Call-Off Contract charges

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

The breakdown of the Charges is:

- Call-Off Contract value: [redacted]
- Payment for period of START DATE – END YEAR 1 is [redacted] comprising:
    - Orgvue Position & Role and Tracking & Monitoring Lenses Subscription [redacted] for the first 12 months
    - Orgvue Activation Services [redacted]
    - Orgvue Professional Services [redacted], including:
      - Aspects of OD configuration & upskill [redacted]
      - Tracking & Monitoring configuration & upskill [redacted]
    - Success Plan – Silver [redacted]
- Payment for period of START OF YEAR 2 – END YEAR 2 is [redacted] (excluding VAT), comprising:
    - Orgvue Position & Role, Tracking & Monitoring and Strategic Workforce Planning Lenses Subscription [redacted] for the second 12 months
    - Success Plan – Silver [redacted]
- Payment for period of START OF YEAR 3 – END YEAR 3 is [redacted] (excluding VAT), comprising:
    - Orgvue Position & Role, Tracking & Monitoring and Strategic Workforce Planning Lenses Subscription [redacted] for the third 12 months
    - Success Plan – Silver [redacted]
- Any travel and subsistence costs for travel outside of central London would be invoiced at cost monthly in arrears in addition to the above.
- Professional Services will be fixed price unless otherwise stated in an agreed Service Description.

Volume Breakdown:

Period	**Positions (Volume)**
19th September 2025 to 18th September 2028	16,500 average, starting at 22,000

	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Orgvue rate card rates are as specified in the G Cloud 14 Service ID 426 303 922 263 495 pricing document under the heading Orgvue additional capability build advisory services, based on the “Skills For the Information Age (SFIA) Rate Card”.

[redacted]

***Note:** As per rate card, the value assigned here is the maximum spend with costs quoted on milestones and paid on delivery. [redacted] to constitute year 1 Activation fees, [redacted] to constitute Tracking and Monitoring configuration and upskill services*

Schedule 3: Collaboration agreement

Not Applicable

Schedule 4: Alternative clauses

Not Applicable

Schedule 5: Guarantee

Not Applicable

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 Clause 2 (Services) 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 Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
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.
Central Government Body	A body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: a. Government Department; b. Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c. Non-Ministerial Department; or d. Executive Agency;
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 UK 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 Call-Off Contract 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)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK 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.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') .
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-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Financial Metrics	The following financial and accounting measures: ● Dun and Bradstreet score of 50 ● Operating Profit Margin of 2% ● Net Worth of 0 ● Quick Ratio of 0.7

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 RM1557.14 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 Clause 2 (Services) 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.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
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 • a Supplier Trigger Event
Intellectual Property Rights or IPR	Intellectual Property Rights are: (a) 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 (b) 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 • (c) 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 Buyer'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, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, 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 Schedule 6.
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.
Performance Indicators	The performance information required by the Buyer from the Supplier set out in the Order Form.
Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK 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 and Performance Indicators 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 Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.
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-controlsche ck-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.
Trigger Event	The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days.
Variation	This has the meaning given to it in clause 32 (Variation process).
Variation Impact Assessment	An assessment of the impact of a variation request by the Buyer completed in good faith, including: a) details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract; b) details of the cost of implementing the proposed variation; c) details of the ongoing costs required by the proposed variation when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure

	required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the variation; and such other information as the Buyer may reasonably request in (or in response to) the variation request;
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Intentionally Blank

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended

Annex 1 - Processing Personal Data

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

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

1.2 The contact details of the Supplier's Data Protection Officer are: [redacted]

[redacted] with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** **The Buyer represents and warrants that in the event it uploads NHSE data, it has the authority to do so** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: ● **Orgvue subscription -** supply of organisation design, HR analytics and workforce planning platform
Duration of the Processing	Duration of the contract and any extension period agreed upon by both parties
Nature and purposes of the Processing	**Nature:** Position and personal data is provided by Buyer for Civil Servants and Contractors. This data is used to produce analysis and model resources in Buyer's organisation. These reports are produced by Buyer and third parties authorised by the Buyer and shared with Buyer's organisational departments.

	Data will be deleted at the end of the contract unless further extension is agreed by both parties. **Purpose:** To optimise Buyer's organisation design, HR analytics and workforce planning and thereby ensure the delivery of the finest public services.
Type of Personal Data	Includes but is not limited to: For DHSC employees and contractors in the workforce • Employee ID • Name • Employment Start Date • Employment End Date • Person Type • Assignment Status • Assignment Status end date • Worker FTE • Office Location (building/city) • Position ID • Cost Centre • Position Description (title) • Position Compensation Level (Grade) • Supervisor Position Description (title) • Supervisor Position ID • Supervisor name (we have to look this up from their Position ID though) • DG Group • Directorate • DD area • Last update date For NHS England employees and contractors in the workforce • Employee Number • Assignment number • Title • First Name • Last Name • Employee Email Address • Employee Person Type • Assignment Category • Assignment Status • Position Number • Position Title • Employee Category • Role • FTE • Employee Location Name • Employee Location Postal Code • Primary Assignment Flag

	• Actual Salary • Full Time Salary • Afc Spinal Point • Grade Step • Payroll Name • Pay Scale • Pay Scale Description • Banding AfC Mappings • Banding Salary Mappings • Position Pay Scale • Position Pay Scale Description • Position AfC Mappings • Employee Latest Start Date • Fixed Term End Date • Employee Original Hire Date • Employee NHS Entry Date • CSD 1 Week • CSD 3 Months • CSD 12 Months • Length of Service (Years) • Supervisor Email • Supervisor Employee Number • Supervisor Name • Assignment Cost Centre • Organisation Cost Centre • Legacy Org • Directorate • Locality/Service • Section • Team • Date of Report
Categories of Data Subject	Staff (including volunteers, agents and temporary workers) and Contract resources
International transfers and legal gateway	EU SCC and UK ITDA.
Plan for return and destruction of the data once the Processing is complete	Supplier to destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so at the end of the contract, or at least within 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.

Annex 2 - Joint Controller Agreement – NOT USED

Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [**select: Supplier or Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for using all reasonable endeavours to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**select:** Supplier's **or Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and Buyer each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Framework Agreement during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Framework Agreement or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) use all reasonable endeavours to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Personal Data Breach having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

(k) where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the destination country has been recognised as adequate by the UK government in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement Addendum to the European Commission's SCCs ("the **Addendum**"), as published by the Information Commissioner's Office from time to time, as well as any additional measures;

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

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

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

(l) where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the transfer is in accordance with Article 45 of the EU GDPR; or

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the

non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures;

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

(iv) the transferring Party complies with its obligations under EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including using such reasonable endeavours as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall use all reasonable endeavours to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of

a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) The Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) The Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Framework Agreement, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Framework Agreement, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Framework Agreement to ensure that it complies with any guidance issued by the Information Commissioner, any relevant Central Government Body and/or any other regulatory authority.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "Claim Losses"):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Buyer shall be entitled to terminate the Framework Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Framework Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Framework Agreement), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Schedule 8 (Corporate Resolution Planning)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Schedule 6 (Glossary and interpretations):

"Accounting Reference Date"	means in each year the date to which the Supplier prepares its annual audited financial statements;
“Annual Revenue”	means, for the purposes of determining whether an entity is a Public Sector Dependent Supplier, the audited consolidated aggregate revenue (including share of revenue of joint ventures and Associates) reported by the Supplier or, as appropriate, the Supplier Group in its most recent published accounts, subject to the following methodology: figures for accounting periods of other than 12 months should be scaled pro rata to produce a proforma figure for a 12 month period; and where the Supplier, the Supplier Group and/or their joint ventures and Associates report in a foreign currency, revenue should be converted to British Pound Sterling at the closing exchange rate on the Accounting Reference Date;

“Appropriate Authority” or “Appropriate Authorities”	means the Buyer and the Cabinet Office Markets and Suppliers Team or, where the Supplier is a Strategic Supplier, the Cabinet Office Markets and Suppliers Team;
“Associates”	means, in relation to an entity, an undertaking in which the entity owns, directly or indirectly, between 20% and 50% of the voting rights and exercises a degree of control sufficient for the undertaking to be treated as an associate under generally accepted accounting principles;
"Cabinet Office Markets and Suppliers Team"	means the UK Government’s team responsible for managing the relationship between government and its Strategic Suppliers, or any replacement or successor body carrying out the same function;
“Class 1 Transaction”	has the meaning set out in the listing rules issued by the UK Listing Authority;

"Control"	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;
"Corporate Change Event"	means: (a) any change of Control of the Supplier or a Parent Undertaking of the Supplier; (b) any change of Control of any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services; (c) any change to the business of the Supplier or any member of the Supplier Group which, in the reasonable opinion of the Buyer, could have a material adverse effect on the Services; (d) a Class 1 Transaction taking place in relation to the shares of the Supplier or any Parent Undertaking of the Supplier whose shares are listed on the main market of the London Stock Exchange plc; (e) an event that could reasonably be regarded as being equivalent to a Class 1 Transaction taking place in respect of the Supplier or any Parent Undertaking of the Supplier; (f) payment of dividends by the Supplier or the ultimate Parent Undertaking of the Supplier Group exceeding 25% of the Net Asset Value of the Supplier or the ultimate Parent Undertaking of the Supplier Group respectively in any 12 month period;

	(g) an order is made or an effective resolution is passed for the winding up of any member of the Supplier Group; (h) any member of the Supplier Group stopping payment of its debts generally or becoming unable to pay its debts within the meaning of section 123(1) of the Insolvency Act 1986 or any member of the Supplier Group ceasing to carry on all or substantially all its business, or any compromise, composition, arrangement or agreement being made with creditors of any member of the Supplier Group; (i) the appointment of a receiver, administrative receiver or administrator in respect of or over all or a material part of the undertaking or assets of any member of the Supplier Group; and/or (j) any process or events with an effect analogous to those in paragraphs (e) to (g) inclusive above occurring to a member of the Supplier Group in a jurisdiction outside England and Wales;
"Corporate Change Event Grace Period"	means a grace period agreed to by the Appropriate Authority for providing CRP Information and/or updates to Business Continuity Plan after a Corporate Change Event;
"Corporate Resolvability Assessment (Structural Review)"	means part of the CRP Information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraph 3 and Annex 2 of this Schedule;

"Critical National Infrastructure" or "CNI"	means those critical elements of UK national infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or significant impact on the national security, national defence, or the functioning of the UK;
"Critical Service Contract"	means the overall status of the Services provided under the Call-Off Contract as determined by the Buyer and specified in Paragraph 2 of this Schedule;
"CRP Information"	means the corporate resolution planning information, together, the: (a) Exposure Information (Contracts List); (b) Corporate Resolvability Assessment (Structural Review); and (c) Financial Information and Commentary

"Dependent Parent Undertaking"	means any Parent Undertaking which provides any of its Subsidiary Undertakings and/or Associates, whether directly or indirectly, with any financial, trading, managerial or other assistance of whatever nature, without which the Supplier would be unable to continue the day to day conduct and operation of its business in the same manner as carried on at the time of entering into the Call-Off Contract, including for the avoidance of doubt the provision of the Services in accordance with the terms of the Call-Off Contract;
"FDE Group" **"Financial Distress Event"**	means the [Supplier, Subcontractors, [the Guarantor] the credit rating of an FDE Group entity dropping below the applicable Financial Metric; an FDE Group entity issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects; there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of an FDE Group entity; an FDE Group entity committing a material breach of covenant to its lenders; a Subcontractor notifying CCS or the Buyer that the Supplier has not satisfied any material sums

	properly due under a specified invoice and not subject to a genuine dispute; any of the following: commencement of any litigation against an FDE Group entity with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m; non-payment by an FDE Group entity of any financial indebtedness; any financial indebtedness of an FDE Group entity becoming due as a result of an event of default; the cancellation or suspension of any financial indebtedness in respect of an FDE Group entity; or the external auditor of an FDE Group entity expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of that FDE entity; in each case which the Buyer reasonably believes (or would be likely to reasonably believe) could directly impact on the continued performance and delivery of the Services in accordance with the Call-Off Contract; and any two of the Financial Metrics for the Supplier not being met at the same time.
"Parent Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Public Sector Dependent Supplier"	means a supplier where that supplier, or that supplier's group has Annual Revenue of £50

	million or more of which over 50% is generated from UK Public Sector Business;
"Strategic Supplier"	means those suppliers to government listed at https://www.gov.uk/government/publications/strategic-suppliers;
"Subsidiary Undertaking"	has the meaning set out in section 1162 of the Companies Act 2006;
"Supplier Group"	means the Supplier, its Dependent Parent Undertakings and all Subsidiary Undertakings and Associates of such Dependent Parent Undertakings;
"UK Public Sector Business"	means any goods, service or works provision to UK public sector bodies, including Central Government Departments and their arm's length bodies and agencies, non-departmental public bodies, NHS bodies, local authorities, health bodies, police, fire and rescue, education bodies and devolved administrations; and

"UK Public Sector / CNI Contract Information"	means the information relating to the Supplier Group to be provided by the Supplier in accordance with Paragraphs 3 to 5 and Annex 1;

2. Service Status and Supplier Status

2.1 This Call-Off Contract [insert 'is' or 'is not'] a Critical Service Contract.

[Guidance: A Critical Service Contract is a service contract which the Buyer has categorised as a Gold contract using the Cabinet Office Contract Tiering Tool available on the Knowledge Hub or which the Buyer, in consultation with the Cabinet Office Markets and Suppliers Team if appropriate, otherwise considers should be classed as a Critical Service Contract.]

2.2 The Supplier shall notify the Buyer and the Cabinet Office Markets and Suppliers Team in writing within 5 Working Days of the Start Date and throughout the Call-Off Contract Term within 120 days after each Accounting Reference Date as to whether or not it is a Public Sector Dependent Supplier. The contact email address for the Markets and Suppliers Team is [redacted]

2.3 The Buyer and the Supplier recognise that, where specified in the Framework Agreement, CCS shall have the right to enforce the Buyer's rights under this Schedule.

3. Provision of Corporate Resolution Planning Information

3.1 Paragraphs 3 to 5 shall apply if the Call-Off Contract has been specified as a Critical Service Contract under Paragraph 2.1 or the Supplier is or becomes a Public Sector Dependent Supplier.

3.2 Subject to Paragraphs 3.6, 3.10 and 3.11:

3.2.1 where the Call-Off Contract is a Critical Service Contract, the Supplier shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the Start Date; and

3.2.2 except where it has already been provided, where the Supplier is a Public Sector Dependent Supplier, it shall provide the Appropriate Authority or Appropriate Authorities with the CRP Information within 60 days of the date of the Appropriate Authority's or Appropriate Authorities' request.

3.3 The Supplier shall ensure that the CRP Information provided pursuant to Paragraphs 3.2, 3.8 and 3.9:

3.3.1 is full, comprehensive, accurate and up to date;

3.3.2 is split into three parts:

(a) Exposure Information (Contracts List);
(b) Corporate Resolvability Assessment (Structural Review);
(c) Financial Information and Commentary

and is structured and presented in accordance with the requirements and explanatory notes set out in the latest published version of the Resolution Planning Guidance Note published by the Cabinet Office Government Commercial Function and available at https://www.gov.uk/government/publications/the-sourcing-and-consultancy-playbooks and contains the level of detail required (adapted as necessary to the Supplier's circumstances);

3.3.3 incorporates any additional commentary, supporting documents and evidence which would reasonably be required by the Appropriate Authority or Appropriate Authorities to understand and consider the information for approval;

3.3.4 provides a clear description and explanation of the Supplier Group members that have agreements for goods, services or works provision in respect of UK Public Sector Business and/or Critical National Infrastructure and the nature of those agreements; and

3.3.5 complies with the requirements set out at Annex 1 (Exposure Information (Contracts List)), Annex 2 (Corporate Resolvability Assessment (Structural Review)) and Annex 3 (Financial Information and Commentary) respectively.

3.4 Following receipt by the Appropriate Authority or Appropriate Authorities of the CRP Information pursuant to Paragraphs 3.2, 3.8 and 3.9, the Buyer shall procure that the Appropriate Authority or Appropriate Authorities shall discuss in good faith the contents of the CRP Information with the Supplier and no later than 60 days after the date on which the CRP Information was delivered by the Supplier either provide an Assurance to the Supplier that the Appropriate Authority or Appropriate Authorities approve the CRP Information or that the Appropriate Authority or Appropriate Authorities reject the CRP Information.

3.5 If the Appropriate Authority or Appropriate Authorities reject the CRP Information:

3.5.1 the Buyer shall (and shall procure that the Cabinet Office Markets and Suppliers Team shall) inform the Supplier in writing of its reasons for its rejection; and

3.5.2 the Supplier shall revise the CRP Information, taking reasonable account of the Appropriate Authority's or Appropriate Authorities' comments, and shall re-submit the CRP Information to the Appropriate Authority or Appropriate Authorities for approval

within 30 days of the date of the Appropriate Authority's or Appropriate Authorities' rejection. The provisions of paragraph 3.3 to 3.5 shall apply again to any resubmitted CRP Information provided that either Party may refer any disputed matters for resolution under clause 32 of the Framework Agreement (Managing disputes).

3.6 Where the Supplier or a member of the Supplier Group has already provided CRP Information to a central government body or the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely to the Cabinet Office Markets and Suppliers Team) and has received an Assurance of its CRP Information from that central government body and the Cabinet Office Markets and Suppliers Team (or, in the case of a Strategic Supplier, solely from the Cabinet Office Markets and Suppliers Team), then provided that the Assurance remains Valid (which has the meaning in paragraph 3.7 below) on the date by which the CRP Information would otherwise be required, the Supplier shall not be required to provide the CRP Information under Paragraph 3.2 if it provides a copy of the Valid Assurance to the Appropriate Authority or Appropriate Authorities on or before the date on which the CRP Information would otherwise have been required.

3.7 An Assurance shall be deemed Valid for the purposes of Paragraph 3.6 if:

3.7.1 the Assurance is within the validity period stated in the Assurance (or, if no validity period is stated, no more than 12 months has elapsed since it was issued and no more than 18 months has elapsed since the Accounting Reference Date on which the CRP Information was based); and

3.7.2 no Corporate Change Events or Financial Distress Events (or events which would be deemed to be Corporate Change Events or Financial Distress Events if the Call-Off Contract had then been in force) have occurred since the date of issue of the Assurance.

3.8 If the Call-Off Contract is a Critical Service Contract, the Supplier shall provide an updated version of the CRP Information (or, in the case of Paragraph 3.8.3 of its initial CRP Information) to the Appropriate Authority or Appropriate Authorities:

3.8.1 within 14 days of the occurrence of a Financial Distress Event (along with any additional highly confidential information no longer exempted from disclosure under Paragraph 3.11) unless the Supplier is relieved of the consequences of the Financial Distress Event as a result of credit ratings being revised upwards;

3.8.2 within 30 days of a Corporate Change Event unless

(a) the Supplier requests and the Appropriate Authority (acting reasonably) agrees to a Corporate Change Event Grace Period, in the event of which the time period for the Supplier to comply with this Paragraph shall be extended as determined by the Appropriate Authority (acting reasonably) but shall in any case be no longer than six months after the Corporate Change Event. During a Corporate Change Event Grace Period the Supplier shall regularly

and fully engage with the Appropriate Authority to enable it to understand the nature of the Corporate Change Event and the Appropriate Authority shall reserve the right to terminate a Corporate Change Event Grace Period at any time if the Supplier fails to comply with this Paragraph; or

(b) not required pursuant to Paragraph 3.10;

3.8.3 within 30 days of the date that:

(a) the credit rating(s) of each of the Supplier and its Parent Undertakings fail to meet any of the criteria specified in Paragraph 3.10; or

(b) none of the credit rating agencies specified at Paragraph 3.10 hold a public credit rating for the Supplier or any of its Parent Undertakings; and

3.8.4 in any event, within 6 months after each Accounting Reference Date or within 15 months of the date of the previous Assurance received from the Appropriate Authority (whichever is the earlier), unless:

(a) updated CRP Information has been provided under any of Paragraphs 3.8.1 3.8.2 or 3.8.3 since the most recent Accounting Reference Date (being no more than 12 months previously) within the timescales that would ordinarily be required for the provision of that information under this Paragraph 3.8.4; or

(b) not required pursuant to Paragraph 3.10.

3.9 Where the Supplier is a Public Sector Dependent Supplier and the Call-Off Contract is not a Critical Service Contract, then on the occurrence of any of the events specified in Paragraphs 3.8.1 to 3.8.4, the Supplier shall provide at the request of the Appropriate Authority or Appropriate Authorities and within the applicable timescales for each event as set out in Paragraph 3.8 (or such longer timescales as may be notified to the Supplier by the Buyer), the CRP Information to the Appropriate Authority or Appropriate Authorities.

3.10 Where the Supplier or a Parent Undertaking of the Supplier has a credit rating of either:

3.10.1 Aa3 or better from Moody's;

3.10.2 AA- or better from Standard and Poors;

3.10.3 AA- or better from Fitch;

the Supplier will not be required to provide any CRP Information unless or until either (i) a Financial Distress Event occurs (unless the Supplier is relieved of the consequences of the Financial Distress Event due to credit ratings being revised upwards) or (ii) the Supplier and its Parent Undertakings cease to fulfil the criteria set out in this Paragraph 3.10, in which

cases the Supplier shall provide the updated version of the CRP Information in accordance with paragraph 3.8.

3.11 Subject to Paragraph 5, where the Supplier demonstrates to the reasonable satisfaction of the Appropriate Authority or Appropriate Authorities that a particular item of CRP Information is highly confidential, the Supplier may, having orally disclosed and discussed that information with the Appropriate Authority or Appropriate Authorities, redact or omit that information from the CRP Information provided that if a Financial Distress Event occurs, this exemption shall no longer apply and the Supplier shall promptly provide the relevant information to the Appropriate Authority or Appropriate Authorities to the extent required under Paragraph 3.8.

4. Termination Rights

4.1 The Buyer shall be entitled to terminate the Call-Off Contract if the Supplier is required to provide CRP Information under Paragraph 3 and either:

4.1.1 the Supplier fails to provide the CRP Information within 4 months of the Start Date if this is a Critical Service Contract or otherwise within 4 months of the Appropriate Authority's or Appropriate Authorities' request; or

4.1.2 the Supplier fails to obtain an Assurance from the Appropriate Authority or Appropriate Authorities within 4 months of the date that it was first required to provide the CRP Information under the Call-Off Contract, which shall be deemed to be an event to which Clause 18.4 applies.

5. Confidentiality and usage of CRP Information

5.1 The Buyer agrees to keep the CRP Information confidential and use it only to understand the implications of an Insolvency Event of the Supplier and/or Supplier Group members on its UK Public Sector Business and/or services in respect of CNI and to enable contingency planning to maintain service continuity for end users and protect CNI in such eventuality.

5.2 Where the Appropriate Authority is the Cabinet Office Markets and Suppliers Team, at the Supplier's request, the Buyer shall use reasonable endeavours to procure that the Cabinet Office enters into a confidentiality and usage agreement with the Supplier containing terms no less stringent than those placed on the Buyer under paragraph 5.1 and incorporated Framework Agreement clause 34.

5.3 The Supplier shall use reasonable endeavours to obtain consent from any third party which has restricted the disclosure of the CRP Information to enable disclosure of that information to the Appropriate Authority or Appropriate Authorities pursuant to Paragraph 3 subject, where necessary, to the Appropriate Authority or Appropriate Authorities entering into an appropriate confidentiality agreement in the form required by the third party.

5.4 Where the Supplier is unable to procure consent pursuant to Paragraph 5.3, the Supplier shall use all reasonable endeavours to disclose the CRP Information to the fullest extent possible by limiting the amount of information it withholds including by:

5.4.1 redacting only those parts of the information which are subject to such obligations of confidentiality;

5.4.2 providing the information in a form that does not breach its obligations of confidentiality including (where possible) by:

(a) summarising the information;

(b) grouping the information;

(c) anonymising the information; and

(d) presenting the information in general terms

5.5 The Supplier shall provide the Appropriate Authority or Appropriate Authorities with contact details of any third party which has not provided consent to disclose CRP Information where that third party is also a public sector body and where the Supplier is legally permitted to do so.

ANNEX 1: EXPOSURE: CRITICAL CONTRACTS LIST

1 The Supplier shall:

1.1 provide details of all agreements held by members of the Supplier Group where those agreements are for goods, services or works provision and:

(a) are with any UK public sector bodies including: central government departments and their arms-length bodies and agencies, non-departmental public bodies, NHS bodies, local buyers, health bodies, police fire and rescue, education bodies and the devolved administrations;

(b) are with any private sector entities where the end recipient of the service, goods or works provision is any of the bodies set out in Paragraph 1.1(a) of this Annex 1 and where the member of the Supplier Group is acting as a key sub-contractor under the contract with the end recipient; or

(c) involve or could reasonably be considered to involve CNI;

1.2 provide the Appropriate Authority with a copy of the latest version of each underlying contract worth more than £5m per contract year and their related key sub-contracts, which shall be included as embedded documents within the CRP Information or via a directly accessible link

ANNEX 2: CORPORATE RESOLVABILITY ASSESSMENT (STRUCTURAL REVIEW)

1. The Supplier shall:

1.1 provide sufficient information to allow the Appropriate Authority to understand the implications on the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 if the Supplier or another member of the Supplier Group is subject to an Insolvency Event;

1.2 ensure that the information is presented so as to provide a simple, effective and easily understood overview of the Supplier Group; and

1.3 provide full details of the importance of each member of the Supplier Group to the Supplier Group's UK Public Sector Business and CNI agreements listed pursuant to Annex 1 and the dependencies between each.

ANNEX 3: Financial information AND COMMENTARY

1 The Supplier shall:

1.1 provide sufficient financial information for the Supplier Group level, contracting operating entities level, and shared services entities' level to allow the Appropriate Authority to understand the current financial interconnectedness of the Supplier Group and the current performance of the Supplier as a standalone entity; and

1.2 ensure that the information is presented in a simple, effective and easily understood manner.

2 For the avoidance of doubt the financial information to be provided pursuant to Paragraph 1 of this Annex 3 should be based on the most recent audited accounts for the relevant entities (or interim accounts where available) updated for any material changes since the Accounting Reference Date provided that such accounts are available in a reasonable timeframe to allow the Supplier to comply with its obligations under this Schedule. If such accounts are not available in that timeframe, to the extent permitted by Law financial information should be based on unpublished unaudited accounts or management accounts (disclosure of which to the Appropriate Authority remains protected by confidentiality).

Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

Contract Details		
This variation is between:	**[insert** name of Buyer] **("the Buyer")** And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation		
Reason for the variation:	**[insert** reason]	
A Variation Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: ● **[Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1 This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

2 Words and expressions in this Variation shall have the meanings given to them in the Contract.

3 The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature .....

Date .....

Name (in Capitals) .....

Address .....