RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	TROO0300
THE BUYER:	Department for Transport (DfT)
BUYER ADDRESS:	Great Minster House, 33 Horseferry Road, London, SW1P 4DR
THE SUPPLIER:	KPMG UK LLP
SUPPLIER ADDRESS:	15 Canada Square, London, E14 5GL
REGISTRATION NUMBER:	OC301540
DUNS NUMBER:	42-391-6167
SID4GOV ID:	N/A

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated: 25th October 2022

It's issued under the Framework Contract with the reference number RM6187 for the provision of specialist strategic consultancy to provide advice and assurance to the High Speed Rail Group on the development and delivery of High Speed 2.

CALL-OFF LOT: Lot 2 Strategy & Policy

Call-off incorporated terms
The following documents are incorporated into this Call-Off Contract.
Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6187

3. The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
- Joint Schedule 9 (Minimum Standards of Reliability)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 3 (Continuous Improvement)
- Call-Off Schedule 5 (Pricing Details)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 15 (Call-Off Contract Management)

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

Supplier terms are not part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

Call-off special terms

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

Special Term 1 - The Buyer is only liable to reimburse the Supplier for any expense or any disbursement which is

(i) specified in this Contract (travel expenses incurred when undertaking the duties for the Construction Inspectorate will be reimbursable) or

(ii) which the Buyer has Approved prior to the Supplier incurring that expense or that disbursement. The Supplier may not invoice the Buyer for any other expenses or any other disbursements

Special Term 2 – With regards to Call Off Schedule 8 Business Continuity and Disaster Recovery, the Supplier will be required to:

(i) ensure that adequate arrangements are put in place to safeguard service delivery under this contract where the Buyer demonstrates by appropriate means that there is a finding against the Supplier of grave professional

misconduct under a UK public contract, which renders its integrity questionable. Such arrangements may include putting in place an assignment of contractual rights granting the Buyer access to the relevant member/s of the Supplier's supply chain for the purpose of business continuity

Call-off start date: 1st November 2022

Call-off expiry date: 31st October 2025

Call-off Optional Extension: End date of Extension Period 1: 31st October 2026
End date of Extension Period 2: 31st October 2027

Call-off deliverables: As per Attachment 3 Statement of Requirements

Security

Short form security requirements apply

and

Section 15 & 16 of Attachment 3 Statement of Requirements

The Supplier will be accountable for data protection ensuring the rights of individuals to personal information is collected and processed and is compliant at all times with the UK General Data Protection Regulation (GDPR).

The Supplier is to note that all staff they supply or intend to supply who have regular access to or will be based at the Employer's premises have complied with the Employer's baseline personnel security standard (BPSS) https://www.gov.uk/government/publications/security-policy-framework.

The Supplier is expected to have secure and robust methodologies for storing and protecting all information related to this project and any other work carried out under this contract.

Due to the highly sensitive nature of the project, the Supplier is required to take adequate steps to ensure suitable protection of, and keep confidential, all information received as part of this contract, including, as necessary, limits on access to IT systems and password protections. There will be serious consequences should any information make its way to the public domain.

The Authority requires that the Supplier treats confidentially all information provided and produced under this contract and that this obligation survives the duration of this contract. The Authority requires that the Supplier produces and maintains robust

processes, systems and controls to ensure information provided and produced under this contract is not shared with third parties or utilised by the Supplier to the benefit of third parties and or to the detriment of the Department.

Maximum liability

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

The Estimated Year 1 Charges used to calculate liability in the first contract year are: £4,800,000 giving a resulting maximum liability of £6,000,000.

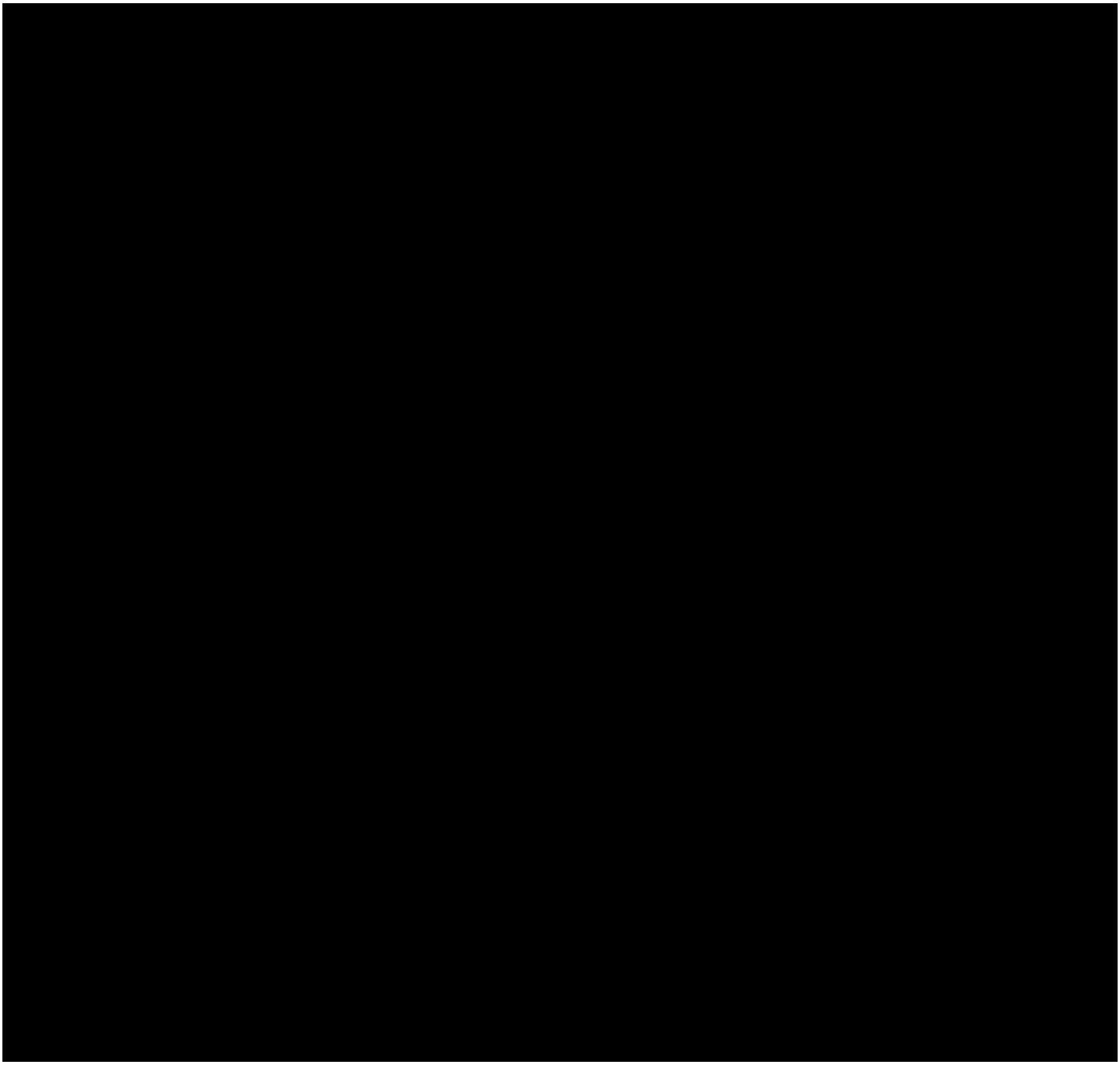
Call-off charges

The total contract value for the initial term (Years 1, 2 & 3) shall not exceed £14,400,000 excluding VAT.

The total estimated contract value for Years 4 & 5 is £4,800,000 each year (£9,600,000 excluding VAT in total). Years 4 & 5 are optional extensions and are subject to the Authority's business needs and supplier performance.

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices).

For the avoidance of doubt, the total contract value for the 5-year period shall not exceed £24,000,000 (excluding VAT).



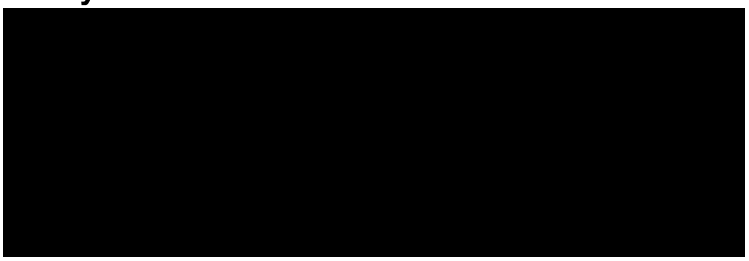
The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law
- Benchmarking using Call-Off Schedule 16 (Benchmarking)

Expenses
As stated in Attachment 3 Statement of Requirements, Section 21, the costs associated with this contract are expected to be covered by the Time and Material fees and the Authority will not pay for travel, meetings rooms and other associated expenses. However, reasonable travel expenses incurred when undertaking the duties for the Construction Inspectorate will be reimbursable.

Payment method
Monthly invoice

Buyer's invoice address



Buyer's authorised representative

Buyer's security policy

Please see Call Off Schedule 9: Security and Section 15 & 16 of Attachment 3

Statement of Requirements

The Supplier will be accountable for data protection ensuring the rights of individuals to personal information is collected and processed and is compliant at all times with the UK General Data Protection Regulation (GDPR).

The Supplier is to note that all staff they supply or intend to supply who have regular access to or will be based at the Employer's premises have complied with the Employer's baseline personnel security standard (BPSS) https://www.gov.uk/government/publications/security-policy-framework.

The Supplier is expected to have secure and robust methodologies for storing and protecting all information related to this project and any other work carried out under this contract.

Due to the highly sensitive nature of the project, the Supplier is required to take adequate steps to ensure suitable protection of, and keep confidential, all information received as part of this contract, including, as necessary, limits on access to IT systems and password protections. There will be serious consequences should any information make its way to the public domain.

The Authority requires that the Supplier treats confidentially all information provided and produced under this contract and that this obligation survives the duration of this contract. The Authority requires that the Supplier produces and maintains robust processes, systems and controls to ensure information provided and produced under this contract is not shared with third parties or utilised by the Supplier to the benefit of third parties and or to the detriment of the Department.

Supplier's authorised representative

[redacted] – [redacted]

Supplier's contract manager

[redacted] – [redacted]

Progress report frequency

The Supplier will be required to report on a number of activities at Contract Management meetings each month and also report on several activities each quarter:

- Preparation for and progress on specified tasks and key actions to be completed per approved Statement of Work (SoW);

- Forward plan on activities per SoW;
- Forecast completion dates for SoW activities;
- Key risks and emerging issues impacting progress across the HS2 Programme with planned or existing mitigations where relevant;
- Financial progress, including costs incurred to date and forecast costs to the end of any particular activity (SoW). This should include activity completed by grade, name of the person who has carried out the work, their daily rate and the total number of hours charged;
- A monthly update of the percentage allocation of grades and weighted day rate for the contract to date against those in the Supplier's Bid;
- Monthly update on the use of SMEs across the Programme;
- Monthly report on knowledge transfer/lessons learned (this can include case studies etc.);
- Quarterly updates on value for money provided by this contract (this can in-clude case studies etc.);
- Final Exit plan to be produced within 3 months of the commencement of the contract and updated annually, with final version in place 1 year before end of contract. A draft exit plan to be provided within a month of contract commencing ;
- Quarterly updates on health and wellbeing in the Contract Workforce, and monthly updates on the use of SMEs if applicable.

Key staff

Department for Transport

[redacted]

[redacted]

KPMG

[redacted]

Key subcontractors
The Nichols Group Ltd

[redacted]

Services to be provided: Support in the provision of assurance and advice to DfT that the development and delivery of HS2 is meeting its requirements and the new railway will be delivered in a manner that will realise the expected benefits and represents value for money for the taxpayer. In particular, technical and engineering and construction input, plus review and challenge of the proposals and performance of HS2 Ltd in respect of costs, time and quality, including delivery of benefits.

Steer Davies & Gleave Ltd

[redacted]

Services to be provided: Support in the provision of assurance and advice to DfT that the development and delivery of HS2 is meeting its requirements and the new railway will be delivered in a manner that will realise the expected benefits and represents value for money for the taxpayer. In particular, technical and engineering and construction input, plus review and challenge of the proposals and performance of HS2 Ltd in respect of costs, time and quality, including delivery of benefits.

Commercially sensitive information

The Supplier is to note that all staff they supply or intend to supply who have regular access to or will be based at the Employer's premises have complied with the Employer's baseline personnel security standard (BPSS) https://www.gov.uk/government/publications/security-policy-framework.

The Supplier is expected to have secure and robust methodologies for storing and protecting all information related to this project and any other work carried out under this contract.

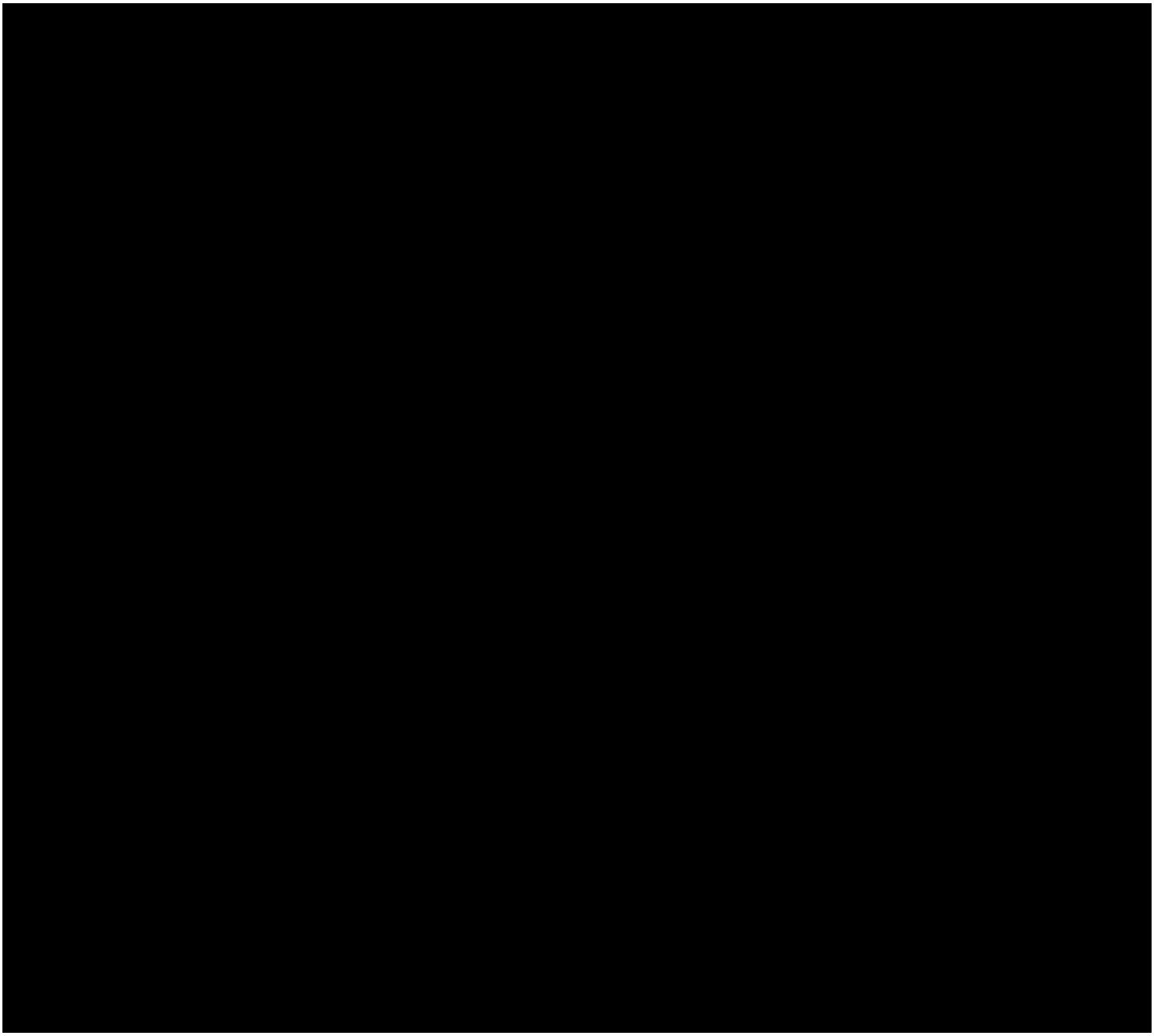
Due to the highly sensitive nature of the project, the Supplier is required to take adequate steps to ensure suitable protection of, and keep confidential, all information received as part of this contract, including, as necessary, limits on access to IT

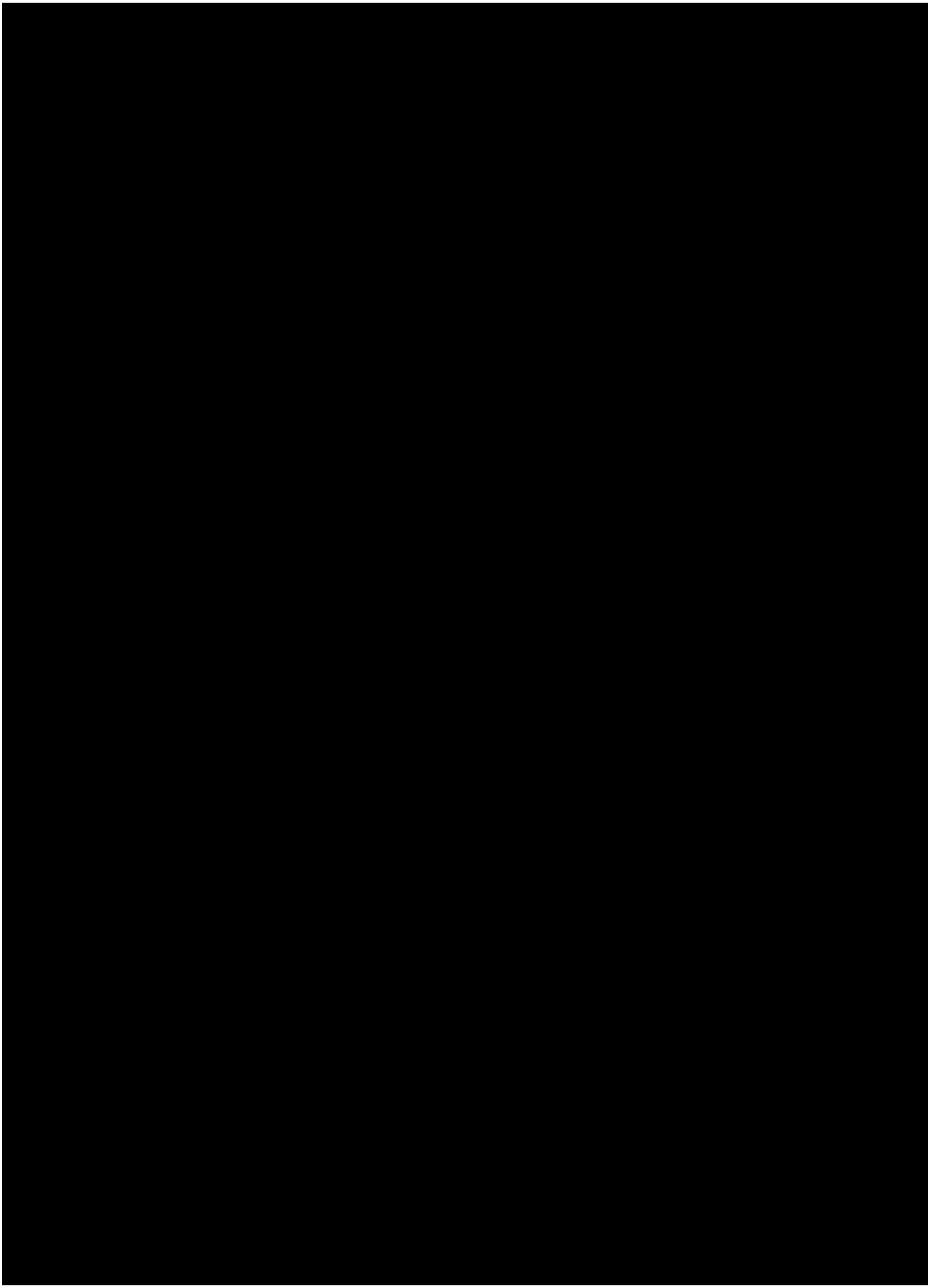
systems and password protections. There will be serious consequences should any information make its way to the public domain.

The Authority requires that the Supplier treats confidentially all information provided and produced under this contract and that this obligation survives the duration of this contract. The Authority requires that the Supplier produces and maintains robust processes, systems and controls to ensure information provided and produced under this contract is not shared with third parties or utilised by the Supplier to the benefit of third parties and or to the detriment of the Department.

Service credits
Not Applicable

Service Levels and Performance





In the event of poor performance through the failure to deliver KPIs to time and of appropriate quality, the Authority shall meet with the Supplier to understand the root cause of the issue. The Supplier shall formulate a Performance Improvement Plan to rectify these issues and meet the requirements in this statement.

If poor performance continues, following formal written warnings, early termination of the Contract will also be considered in line with the Framework Terms and Conditions.

The Authority will discuss the KPI scorecard and commentary at Contract Management meetings with the Supplier. The Authority will measure performance using the Key Performance Indicators above. Each month the Supplier will be

required to complete the section 'Supplier Reported Performance' and a proposed score and provide it to the Contract Manager 5 working days before the Contract Management meeting. A final score and commentary will be agreed by both parties in the meeting. The KPI scorecard will be provided to the Supplier at the inception meeting.

The Authority mandates that DfTc and Executive Agencies shall publish three top KPIs relating to their 'most important' contracts, as per the Sourcing Playbook. The purpose of publishing 3 top KPIs from the DfT's 'most important' contracts is to build trust in the delivery of public services and increase transparency. Furthermore, it is a requirement of the government's transparency agenda (as evidenced in the Sourcing Playbook) that three KPIs from each of the government's most important contracts shall be made publicly available. The Authority will identify the most important contracts to publish and will inform Suppliers of the publication. The Supplier must ensure that they report on their KPIs on a monthly basis using the KPI scorecard template which will be provided at the Inception meeting. The Authority also reserves the right to publish KPIs with no further notice to the Supplier.

Notwithstanding any other term of this Contract, the Supplier hereby gives consent for the Authority to publish to the general public the Contract (and any documents subsequently produced by either party as part of management of the contract – including, but not limited to, performance against key performance indicators and plans to rectify the same etc.) in their entirety, including from time to time agreed changes to the Contract.

Additional insurances
Not Applicable

Guarantee
Not Applicable

Buyer's environmental and social value policy

The Supplier is expected to demonstrate how they promote principles of Social Value in their organisation, which will include activities that:

- Demonstrate action to support the health and wellbeing, including physical and mental health, in the contract workforce.

- Demonstrate action to create a diverse supply chain to deliver this contract which includes SMEs.

Social value commitment
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off

Schedule 4 (Call-Off Tender).

Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

For and on behalf of the Supplier:

Signature [redacted]

Name:

Role: KPMG Partner

Date: 26 October 2022

For and on behalf of the Buyer:

Signature: [redacted]

Name:

Role:

Date:

Annexes

- Annex A: MCF3 Terms and Conditions
- Annex B: Supplier Bid Proposal

Included as separate attachments

Joint Schedule 11 (Processing Data)

Definitions

o In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

Status of the Controller

o The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- "Controller" in respect of the other Party who is "Processor";
- "Processor" in respect of the other Party who is "Controller";
- "Joint Controller" with the other Party;
- "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

o Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

o The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

o The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

- a systematic description of the envisaged Processing and the purpose of the Processing;
- an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

- an assessment of the risks to the rights and freedoms of Data Subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

o The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

- Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
- ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
    - nature of the data to be protected;
    - harm that might result from a Personal Data Breach;
    - state of technological development; and
    - cost of implementing any measures;
- ensure that :
    - the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
    - it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
        - o are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
        - o are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
        - o are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
        - o have undergone adequate training in the use, care, protection and handling of Personal Data;
- not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

- the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
- the Data Subject has enforceable rights and effective legal remedies;
- the Processor 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 Controller in meeting its obligations); and
- the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

▪ at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

o Subject to paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

▪ receives a Data Subject Access Request (or purported Data Subject Access Request);

▪ receives a request to rectify, block or erase any Personal Data;

▪ receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

▪ receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

▪ receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

▪ becomes aware of a Personal Data Breach.

o The Processor's obligation to notify under paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

o Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

- the Controller with full details and copies of the complaint, communication or request;
- such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
- the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- assistance as requested by the Controller following any Personal Data Breach; and/or
- assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

o The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

- the Controller determines that the Processing is not occasional;
- the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
- the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

o The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

o The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

o Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

- notify the Controller in writing of the intended Subprocessor and Processing;
- obtain the written consent of the Controller;
- enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
- provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

o The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

o The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an

applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

- The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

- In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

Independent Controllers of Personal Data

- With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

- Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

- Where a Party has provided Personal Data to the other Party in accordance with paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

- The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

- The Parties shall only provide Personal Data to each other:

  - to the extent necessary to perform their respective obligations under the Contract;

  - in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

  - where it has recorded it in Annex 1 *(Processing Personal Data).*

- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational

measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

- A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

- Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

  - the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

  - where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

    - promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

    - provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

- Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

  - do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

  - implement any measures necessary to restore the security of any compromised Personal Data;

  - work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

  - not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

- Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

- Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

- Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 28 of this Joint Schedule 11.

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 Relevant Authority at its absolute discretion.

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer [redacted]

1.1.1.2 The contact details of the Supplier's Data Protection Officer are:

[redacted]

1.1.1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Business contact details of Supplier Personnel for which the Supplier is the Controller, • Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller
Duration of the Processing	For the duration of the Framework Contract plus 7 years
Nature and purposes of the Processing	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]

Type of Personal Data	• Full name • Workplace address • Workplace Phone Number • Names • Job Title • Compensation • Tenure Information Qualifications or Certificate • Nationality • Education and Training History • Personal Interests • References and referee details • National Insurance Number • Bank statement • Utility bills • Job title or role • Job application details • Start date • End date and reason for termination • Contract type • Compensation data • Photographic Facial Image • Biometric data • Birth certificates • IP address • Details of physical and Psychological health or medical condition • Next of kin & emergency contact details • Record of absence, time tracking & annual leave
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	For the duration of the Framework Contract plus 7 years

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

- **Definitions**

i. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"BCDR Plan"	has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);
"Disaster Recovery Deliverables"	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	has the meaning given to it in Paragraph 6.3 of this Schedule;

7. **BCDR Plan**

i. The Buyer and the Supplier recognise that, where specified in Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

ii. At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

i. ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables;

ii. ensure the recovery of the Deliverables in the event of a Disaster; and

iii. ensure that adequate arrangements are put in place to safeguard service delivery under this contract where the Buyer demonstrates by appropriate means that there is a finding against the Supplier of grave professional misconduct under a UK public contract, which renders its integrity questionable. Such arrangements may include putting in place an assignment of contractual rights granting the Buyer access to the relevant member/s of the Supplier's supply chain for the purpose of business continuity.

iii. The BCDR Plan shall be divided into three sections:

i. Section 1 which shall set out general principles applicable to the BCDR Plan;

ii. Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

iii. Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

iv. Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree on the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Disputes shall be resolved in accordance with the Dispute Resolution Procedure.

8. **General Principles of the BCDR Plan (Section 1)**

i. Section 1 of the BCDR Plan shall:

i. set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

ii. provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

iii. contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

iv. detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Suppliers in each case as notified to the Supplier by the Buyer from time to time;

v. contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

vi. contain a risk analysis, including:

1. failure or disruption scenarios and assessments of likely frequency of occurrence;

2. identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

3. identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

4. a business impact analysis of different anticipated failures or disruptions;

vii. provide for documentation of processes, including business processes, and procedures;

viii. set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

ix. identify the procedures for reverting to "normal service";

x. set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

xi. identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

xii. provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

ii. The BCDR Plan shall be designed so as to ensure that:

i. the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

ii. the adverse impact of any Disaster is minimised as far as reasonably possible;

iii. it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

iv. it details a process for the management of disaster recovery testing.

iii. The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

iv. The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service Levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

9. **Business Continuity (Section 2)**

i. The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

   i. the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

   ii. the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

ii. The Business Continuity Plan shall:

   i. address the various possible levels of failures of or disruptions to the provision of Deliverables;

   ii. set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

   iii. specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

   iv. set out the circumstances in which the Business Continuity Plan is invoked.

10. **Disaster Recovery (Section 3)**

i. The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

ii. The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

   i. loss of access to the Buyer Premises;

   ii. loss of utilities to the Buyer Premises;

   iii. loss of the Supplier's helpdesk or CAFM system;

   iv. loss of a Subcontractor;

   v. emergency notification and escalation process;

   vi. contact lists;

   vii. staff training and awareness;

   viii. BCDR Plan testing;

ix. post implementation review process;

x. any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

xi. details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

xii. access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

xiii. testing and management arrangements.

11. Review and changing the BCDR Plan

i. The Supplier shall review the BCDR Plan:

i. on a regular basis and as a minimum once every six (6) Months;

ii. within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

iii. where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

ii. Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

iii. The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

iv. Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree on the Review Report

and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Disputes shall be resolved in accordance with the Dispute Resolution Procedure.

v. The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practises or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

12. **Testing the BCDR Plan**

i. The Supplier shall test the BCDR Plan:

  i. regularly and in any event not less than once in every Contract Year;

  ii. in the event of any major reconfiguration of the Deliverables

  iii. at any time where the Buyer considers it necessary (acting in its sole discretion).

ii. If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

iii. The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

iv. The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved by the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

v. The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

  i. the outcome of the test;

  ii. any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

  iii. the Supplier's proposals for remedying any such failures.

vi. Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

13. **Invoking the BCDR Plan**

i. In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

14. **Circumstances beyond your control**

i. The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.