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

Order Form

CALL-OFF REFERENCE:	TROP0104
THE BUYER:	Department for Transport
BUYER ADDRESS	Great Minster House, 33 Horseferry Road, London, SW1P 4DR
THE SUPPLIER:	[redacted]
SUPPLIER ADDRESS:	[redacted]
REGISTRATION NUMBER:	[redacted]
DUNS NUMBER:	[redacted]
SID4GOV ID:	[redacted]

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated: 11 September 2024

It's issued under the Framework Contract with the reference number RM6187 for the provision of Financial Advisors for the Rolling Stock Advisory Team (RAT).

CALL-OFF LOT: Management Consultancy Framework 3 (MCF3) Lot 4 Finance.

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 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 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

Special Term 1:

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 purposes of business continuity.*

Call-off start date: 16 September 2024

Call-off expiry date: 15 September 2026

Call-off initial period: 24 months with an option to extend for an additional 12 months at the Authority's sole discretion and subject to further budgetary approval.

Call-off optional extension: 12 months

End date of extension period 1: 15 September 2027

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

Security

Short form security requirements apply

and

The Authority takes data security extremely seriously and applies agreed government security procedures to all Contracts involving the handling of data and 'Official Sensitive' and 'Commercial Sensitive' information.

There are no specific security requirements, however in line with standard procedure it is expected that the Potential Provider has 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 Potential Provider is required to take adequate steps to ensure suitable protection of, and keep confidential, all information received as part of the Scope of Work, 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 Potential Provider 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 Potential Provider 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 Potential Provider to the benefit of third parties and or to the detriment of the Department.

Potential Providers are to note that all staff they supply or intend to supply who have regular access to or will be based at the Authority's premises have complied with the Authority's Baseline Personnel Security Standard (BPSS).

(https:/www.gov.uk/government/publications/security-policy-framework)

Please also see Annex A – Information and Cyber Security Policy

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: £140,000 giving a resulting maximum liability of £175,000

Call-off charges

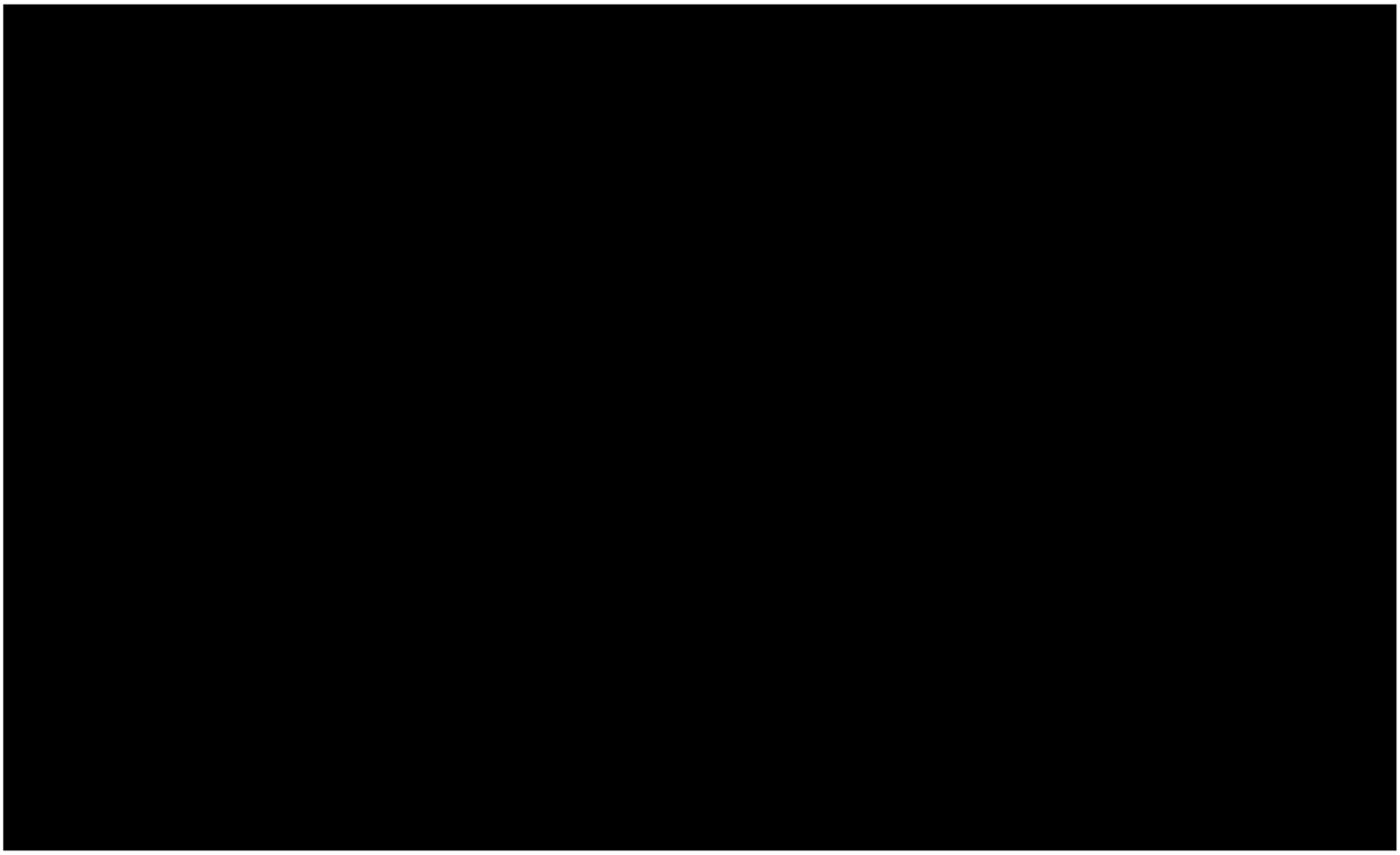
The total contract value is up to £300,000 excluding VAT.

The option to extend is at the Authority's sole discretion and subject to approvals.

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)

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)



Reimbursable expenses

The costs associated with this contract are expected to be covered by the Time and Materials fees and the Authority will not pay for travel, meetings rooms and other associated expenses.

Payment method

Monthly invoice

Buyer's invoice address

DfT Shared Services Arvato
Accounts Payable Team
5 Sandringham Park
Swansea Vale

Swansea
SA7 0EA
support@ubusinessservices.co.uk

FINANCIAL TRANSPARENCY OBJECTIVES
The Financial Transparency Objectives **do not** apply to this Call-Off Contract.

Buyer's authorised representative
[redacted]

Buyer's security policy
DfT's Information and Security Policy – Please see Annex A

Supplier's authorised representative
[redacted]

Supplier's contact manager
[redacted]

Progress report frequency
The Authority expects the Potential Provider to provide progress reports monthly and as may reasonably be required by the Authority from time to time. Such reports would be expected to cover the following:

- Progress on milestones and deliverables and actions to be completed
- Key risks and emerging issues with planned mitigations where relevant
- Financial progress including costs incurred to date, forecast costs to the end of any particular work stream activity. This should include a detailed breakdown of activity completed by grade, hours charged together with the name of the person who has carried out the work and their daily rate.
- A monthly update of the percentage allocation of grades and weighted day rates for the contract to date against those in the Potential Provider's Bid
- Quarterly report on knowledge transfer/lessons learned (this can include case studies etc.)
- Quarterly updates on health and wellbeing in the Contract Workforce (social value)
- Exit plan to be produced at the start of the contract and updated annually with a final version in place 1 year before the end of the contract. A draft exit plan to be provided within 1 month of the contract start date

Progress meeting frequency
Formal contract management review meetings will be held monthly at pre-agreed dates by Microsoft Teams meetings or at Great Minster House.

At the meeting the scorecard and commentary will be discussed, and the Potential Provider will be required to complete the scorecard 5 days ahead of the Contract Management meeting as described in Section 14.

Attendance at Contract Review meetings shall be at the Supplier's own expense. Variations required to the contract or sub-contracts will be undertaken by the use of the variation notice at Joint Schedule 2: variation form v4.1 in the Management Consultancy Framework Three (MCF3) document suite. This can be found on the Crown Commercial Website.

The Financial Advisors are expected to raise and escalate significant or unresolved risks and issues to the appropriate level of authority within the advisor, up to and including Partners or Directors, and raise such risks and issues directly with the Authority's Client Contract Manager.

The Authority will appoint a Contract Manager to manage this contract.

Key staff

[redacted]

Key subcontractor(s)
N/A

Commercially sensitive information

The Authority takes data security extremely seriously and applies agreed government security procedures to all Contracts involving the handling of data and 'Official Sensitive' and 'Commercial Sensitive' information.

There are no specific security requirements, however in line with standard procedure it is expected that the Potential Provider has 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 Potential Provider is required to take adequate steps to ensure suitable protection of, and keep confidential, all information received as part of the Scope of Work, 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 Potential Provider 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 Potential Provider 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 Potential Provider to the benefit of third parties and or to the detriment of the Department.

Additional insurances
Not applicable

Guarantee
Not applicable

Key Performance Indicators

See below

KPI/SLA	Service Area	KPI/SLA description	Target	Weighting
1	Deliverables	Overall Project Deliverables: • How satisfied is the Client with the delivery of the services from the Supplier? • Have all the deliverables been met in accordance	Score of 8+/10	25%

		with the requirements and expectations on quality?		
2	Staff	Staff Competence: • How satisfied is the Client with the Supplier's staff appointed to the project competent and suitably qualified to perform the work required of them by the project? • Do the staff communicate effectively, attend regular meetings / conference calls and follow-up accordingly, as required by the project? • Are the staff's deliverables consistent with the required reporting / evaluations expected by the Client team? Where SME's are engaged, has the competency and performance of the staff from the SME met with the required expectations?	Score of 8+/10	20%
3	Mobilisation and Delivery to Programme / Project Deadlines	• Has the Supplier mobilised in a manner consistent with the Client team's expectations? • How satisfied is the Client with the programme management by the Supplier?	Score of 8+/10	20%

		• Has the Supplier suitably managed project deliverables in a timely manner? If not, has the Supplier provided suitable notice of any possible delays to the programme and/or identified suitable corrective action and acted accordingly? • Is the Client satisfied that the overall programme is under control		
4	Project Budget Management	• The Client is responsible for the internal reporting on project costs, which is supported by regular Consultant updates on billing and forecasts • How satisfied is the Client with the Consultant's billing processes and forecast updates? Is the Client satisfied that it clears GRN's and the Department duly pays the approved invoices?	Score of 8+/10	15%
5	Knowledge Transfer	• How satisfied is the Authority with the Supplier's approach to knowledge transfer? • Has the Supplier delivered suitable standards of knowledge transfer where it has been undertaken? • Has there been appropriate knowledge transfer on elements that	Score of 8+/10	10%

		would be relevant to closure and exit of the contract?		
6	Social Value	• Has the Supplier provided satisfactory updates on actions to invest in the physical and mental health and wellbeing of the contract workforce	Score of 8+/10	5%
7	Exit Strategy	• Has the Supplier passed onto the RISDG team as part of the exit process all information required for future use, therefore, enabling the project to be closed off with no outstanding dependencies? • Has the Supplier provided the draft Exit Plan within one month of the contract commencing? • Has the Supplier provided an annual Exit Plan (from contract commencement date) and updated exit plans?	Score of 8+/10	5%

A scoring system of 0-10 is used to assess the Supplier's performance in each of the areas measured:

0 = Completely Dissatisfied
2 = Highly Dissatisfied
4 = Mildly Dissatisfied
6 = Mildly Satisfied
8 = Highly Satisfied
10 = Completely Satisfied

Successful consultants should note that the weighting included in the above KPI table are part of the Contract Management process and it is not related to the evaluation process in any way.

In the event of poor performance through the failure to deliver KPIs to time and of appropriate quality, the Authority shall meet with the Successful consultant to understand the root cause of the issue. The Successful consultant shall formulate a Performance Improvement Plan, in agreement with the Authority, 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 Successful consultant. The Authority will measure performance using the Key Performance Indicators above. Each month the Successful consultant 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 template is attached with the ITT pack.

The Cabinet Office 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 Cabinet Office will identify the most important contracts to publish and will inform Suppliers of the publication. The Successful consultant 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 Cabinet Office also reserves the right to publish KPIs with no further notice to the Successful consultant.

Notwithstanding any other term of this Contract, the Successful consultant 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.

Buyer's environmental and social value policy

- DfT Corporate Environmental Policy – Please see Annex B

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: [redacted]

Role: [redacted]

Date: 24/09/2024

For and on behalf of the Buyer:

Signature: [redacted]

Name: [redacted]

Role: [redacted]

Date: 19 /09 /2024

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.

- 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:
      - 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;
      - are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
      - 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
      - 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.

- 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.

- 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.

- 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.

- 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).

o 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

o 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

o 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.

o 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 are: [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

Annex A – DfT's Information and Cyber Security Policy

1. Introduction

The Department for Transport Central (DfTc) Information & Cyber Security Policy Framework provides an overview of Digital Services suite of Information Security policies. The policies set out the minimum requirements for information security which the Department, its delivery partners and third party suppliers must comply.

2. Purpose

The purpose of this policy is to demonstrate the management board's commitment to Information Security and to support the overarching policy principles to which all subordinate policies and controls must adhere to. It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity and availability of information.

3. Objectives

The aim of this policy is to enable and maintain effective information security through implementing supporting policies, standards and controls to protect information assets processed or stored by and on behalf of DfTc.

The key objectives of the Departmental Information & Cyber Security Policy Framework are the preservation of confidentiality, integrity, and availability of systems and information. These three pillars compose of the Confidentiality, Integrity, Availability triad:

- **Confidentiality** - Access to information shall be restricted to those authorised users with a legitimate business need and appropriate authority to view it.
- **Integrity** – Data and information are to be complete and accurate with all management systems operating correctly.
- **Availability** - Information shall be readily available to those authorised to view it as and when it is needed.

This objective can be achieved through safeguarding the Confidentiality, Integrity and

Availability of DfTc Assets and all information it collects, stores, transfers and process for clients, staff and partners in accordance with legislation, regulation and contractual obligations.

4. Scope

DfTc's Information & Cyber Security Policy Framework shall apply to all data, information, information systems, networks, applications, devices, locations used to store, process, transmit or receive information and staff within DfTc, its primary delivery partners and third-party suppliers.

Never-the-less the scope shall be based on and remain compliant with the mandatory requirements set out within the Minimum Cyber Security Standard.

5. Overarching Principles

DfTc is committed to protecting the security of its information and information systems against breaches of confidentiality, failures of integrity or interruptions to the availability.

In order to meet this intent, DfTc will adopt the overarching principles below:

- ensure that senior management provides clear direction to imbed information security within all DfTc's strategic objectives to deliver secure and successful services
- ensure compliance with legal, statutory, regulatory or contractual obligations related to information security
- establish a management framework to initiate and control the implementation and operation of information security
- implement human, organisational, and technological security controls to preserve the confidentiality, availability and integrity of its information systems
- develop and maintain policies, procedures and guidelines to meet government standards for information security, reflecting industry best practice
- ensure robust risk management processes are in place to identify potential threats, vulnerabilities and controls to reduce the risks to an acceptable level
- ensure that staff and contractors understand their responsibilities in relation to information security
- ensure information security is an integral part of information systems throughout its lifecycle (from concept to disposal/termination)
- ensure access to information and information assets is granted on the need to know principle
- ensure policy and controls on remote working practices and the use of removable media for legitimate business purposes are in place and documented
- ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

- keep up to date on latest cyber security threats and trends through various reliable sources and apply good working practices
- continuously review and improve DfTc's information security controls to minimise and prevent compromise to information systems
- establish information security education, training and awareness initiatives, ensuring that all users conduct mandatory information security awareness training
- ensure that information security is implemented and operated in accordance with this policy and other supporting, policies, procedures or standards
- ensure independent reviews of information security policy and associated controls are performed internally and using services of an external/third party reviewer annually

6. Responsibilities for Information Security

Overall responsibility for information security and assets shall rest with the Business.

Heads of Departments shall ensure that information security within their business area shall promote good information and cyber security practices and ensure that staff adhere to DfTc's Information & Cyber Security Policies Framework.

The Senior Information Risk Owner is responsible for the direction of information risk at board level and takes the lead in the departments strategic approach for managing risks, supported by the Head of Information & Cyber Security.

Head of Information and Cyber Security will be the owner for all Information & Cyber Security Policies within DfTc.

On a day-to-day basis the Digital Assurance Manager shall be responsible for organising and managing information and cyber security; ensuring the department is abreast of all related security policies and good working practices.

Digital Services has overall responsibility for creating, updating, reviewing (annually) and disseminating the suite of Information & Cyber Security Polices as well as providing staff training and awareness on Information & Cyber Security.

Line Managers shall be responsible for ensuring that staff, contractors and third party users are aware of and apply:

- The information security policy suite
- Their personal responsibilities for information security
- Who to ask for further advice on information security matters

Users are responsible for complying with the terms of this policy and all DfTc policies, procedures, regulations and legislation governing the information and systems they access.

7. Compliance and Breach of Policy

DfTc shall conduct and maintain cyber security compliance and assurance activities on the subordinate polices to effectively manage information risks and ensure cyber security objectives and the requirements of the policy are met.

All staff shall abide by the security policies of the Department. Staff shall remain responsible for both the security of their immediate working environments and for security of the data, information assets, systems and devices they use, ensuring that their confidentiality and integrity are not breached, and their proper availability is maintained. Failure to do so may result in disciplinary action.

If you have any questions or concerns about this policy, please discuss them with your line manager.

8. Review and Development

This Information & Cyber Security Policy Framework shall be owned, maintained, reviewed and updated by Information and Assurance team. The suite of Information Security Policies shall be owned, maintained, reviewed and updated by Digital Services. This review shall take place annually or in response to changes in service, technology. Reviews will account for changes to legislation and regulations.

9. Associated Documentation

This overarching policy provides direction for all DfTc information security policies, standards and controls which underpin it.

DfTc's Information Security Policy Framework is underpinned by a suite of Information & Cyber Security policies. Details of which can be found within the table below in **Appendix A**.

All staff, users, and any third parties authorised to access the DfTc network or information systems are required to familiarise themselves with these supporting policies and to adhere to them.

Appendix A: associated documentation

Policies supporting this framework include (this is not an exhaustive list):

Policy	Summary

Acceptable Use Policy	The Acceptable Use Policy (AUP) aims to protect all users of DfTc equipment and data and minimise risk by providing clarity on the behaviours expected and required by DfTc Staff, Agents, Service Providers, Contractors and Consultants. It sets a framework on how to conduct DfTc's business to meet legal, contractual, and regulatory requirements and defines how individuals must behave in order to comply with this policy.

Information Security Governance Framework	The purpose of this policy is to demonstrate the management board's commitment to Information Security. It sets out a framework of governance and accountability for information security management across DfTc and forms the basis of DfTc's Information Security Management System (ISMS). This incorporates all policies, standards and procedures that are required to protect DfTc's data and information.
Information and Cyber Security Policy Framework	The purpose of this policy is to support the overarching policy principles to which all subordinate policies and controls must adhere to. It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity, and availability of information. It includes a set of policies for information and cyber security which are defined, approved by management, published, communicated, and understood by staff, partners, and external parties.
Privilege Account Policy	This policy details the measures that must be in place for the management of privileged accounts which operate across the Department for Transport central (DfTc) estate.
Information Risk Management Policy (Medium)	This policy details the importance of creating a culture that actively manages risk, how the Department wishes to embed risk management into decision making and the risk appetite of the Department. It also details the various roles and responsibilities of individuals, the requirements for recording risks and the departmental risk process.
Information Risk Management Framework (Medium)	The risk management framework enables DfTc to apply the principles and best practices of risk management to improving the security of its systems and critical infrastructure within desired levels across DfTc in line with strategy and risk appetite to achieve its objectives.

Information Asset Policy	This policy sets out DfTc's approach to managing data within information assets in accordance with their classification and value. It explains the concept of an Information Asset and defines the role of the Information Asset Owner who is responsible for each Information Asset. This policy also sets out the primary responsibilities of an Information Asset Owner for managing the risks to personal data and business critical information held within a department.
Joiner, Movers, Leavers Policy	This policy outlines the security requirements associated with any individuals who join, move within, work for, or leave the DfTc.
Secure Configuration Policy	This policy provides guidelines for applying effective, secure, and reliable configuration management techniques, whether in test, development, or production environments. Outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the company security/network security environment.

Patch Management Policy	This policy is comprised of a set of steps and procedures aimed towards managing and mitigating vulnerabilities within the DfTc environment through a regular and well- documented patching process.
Vulnerability Management Standard	This standard sets out the requirement to identify and address technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in security breaches and damage to DfTc reputation.
Managed Device Policy	This policy provides guidance to staff who intend to use their own smartphones, tablets, laptops, and desktop PCs to access work information and services.
Bring Your Own Device Policy (BYOD)	This policy sets out requirements for the use of personally owned devices for work purposes to ensure systems and data are accessed and used appropriately, legally, and securely and staff clearly understand their responsibilities when using BYOD.
Password Policy	This policy defines the standard for creation and management of strong passwords.
Removable-Media Policy	This policy establishes the principles and working practices that are to be adopted by staff of the Department for Transport Central (DfTc) in relation to the use of removable media for data transfer. It also details the measures that must be in place to ensure the controlled use of removable media devices where a valid business case for its use has been provided.
Overseas Working Policy	This policy outlines the principles and working practices that are to be adopted by all staff posted outside of the United Kingdom whilst working for DfTc.

Supplier Assurance Framework/Policy	This policy sets out the requirements when engaging with third-party suppliers who have access to any DfTc information assets. It provides guidance on identifying and managing risks through assessments and monitoring third party compliance with business standards.
Access Control Policy	This policy outlines the requirements for the management of access control to minimise potential exposure from unauthorised access to resources and ensure that only authorised individuals have access to networks, systems and applications, to preserve and protect confidentiality, integrity and availability.
Account Management Policy	The purpose of this policy is to establish the requirements and processes to protect, monitor, and audit account access and reduce the compromise of user accounts by reducing the attack surface.
Authentication Policy	This policy sets out the principles and responsibilities for the identification and authentication of users and devices for accessing DfTc data and/or services to protect against a security breach by verifying that each user is who they claim to be and restricting access to authorised users.
Information Security Exception Policy	This policy explains how an exception request for deviation from the normal or non-compliance to any cyber security polices and standards can be requested, and the required process for effective management of expectations to mitigate risk.

Annex B – DfT Corporate Environmental Policy

Policy statement

DfT is committed to protecting the environment, reducing pollution and whole life carbon in our procurements and continually improving our environmental performance.

Scope

This policy applies to the Department for Transport central department. Any DfT arms-length bodies or executive agencies may use this policy or apply their own.

Description

DfT's operational activities and the individual activity of its staff affect the environment.

The aim of this policy is to inform our interested parties including staff, contractors, suppliers and the public that DfT is committed to reducing any negative environmental impacts produced by our activities, products and services.

Our policy is to continually improve our environmental performance by:

- reducing our greenhouse gas emissions from energy use
- reducing waste and maximising reuse and recycling
- reducing our greenhouse gas emissions from business travel
- controlling how much water we use
- reducing how much paper we use
- protecting our biodiversity and ecosystems
- adapting to climate change
- reducing the carbon impact of our construction projects through innovative methods, cleaner materials and more efficient design

Delivery and monitoring

We will:

- fulfil our compliance obligations in relation to the environment
- meet or exceed the terms of the government's policy on the environment
- set targets to reduce our environmental footprint and protect the environment
- collate, monitor, and analyse data to measure performance against our targets
- prepare for policy changes and tighter targets
- encourage staff, contractors and suppliers to reduce their impact on the environment when providing services and products to us and within their own organisations
- report progress against our targets quarterly to a senior performance board
- report our environmental performance openly and transparently through our annual report and accounts

Although the Department is responsible for the environmental performance of DfT,

we expect all staff, contractors and suppliers involved in DfT's business to share this responsibility.