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

Order Form

CALL-OFF REFERENCE:	con_25114
CALL-OFF TITLE:	Legal Aid Agency Digital Transformation Programme - Assess Civil Applications Service (Decide) and Digital Delivery Services
CALL-OFF CONTRACT DESCRIPTION:	Legal Aid Agency Digital Transformation Programme - Assess Civil Applications Service (Decide) and Digital Delivery Services
THE BUYER:	Secretary of State for Justice, on behalf of the Crown
BUYER ADDRESS	Ministry of Justice, 102 Petty France, London, SW1H 9AJ
THE SUPPLIER:	Made Tech Limited
SUPPLIER ADDRESS:	Fora, 35-41 Folgate Street, London, England, E1 6B
REGISTRATION NUMBER:	06591591
DUNS NUMBER:	211199050
SID4GOV ID:	N/A

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 10 June 2025.

It's issued under the Framework Contract with the reference number RM6263 for the provision of Digital Specialists and Programmes Deliverables.

The Parties intend that this Call-Off Contract will not, except for the first Statement ofWork which shall be executed at the same time that the Call-Off Contract is executed, oblige the Buyer to buy or the Supplier to supply Deliverables.

The Parties agree that when a Buyer seeks further Deliverables from the Supplier under the Call-Off Contract, the Buyer and Supplier will agree and execute a further Statement of Work (in the form of the template set out in Annex 1 to this Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules).

Upon the execution of each Statement of Work it shall become incorporated into the Buyer and Supplier's Call-Off Contract.

CALL-OFF LOT(S): Lot 1 Digital Programmes.

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict,the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions) RM6263
3. Framework Special Terms
4. The following Schedules in equal order of precedence:

    - Joint Schedules for RM6263
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 7 (Financial Difficulties) – **Not Used**
        - Joint Schedule 8 (Guarantee) – **Not Used**
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)
        - Joint Schedule 12 (Supply Chain Visibility)
        - Joint Schedule 13 (Cyber Essentials)

    - Call-Off Schedules for RM6263
        - Call-Off Schedule 1 (Transparency Reports)
        - Call-Off Schedule 2 (Staff Transfer) – Part C and E
        - Call-Off Schedule 3 (Continuous Improvement)
        - Call-Off Schedule 5 (Pricing Details and Expenses Policy)

- Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliveries)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- Call-Off Schedule 9 (Security) – **Short Form**
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 12 (Clustering) – **Not Used**
- Call-Off Schedule 13 (Implementation Plan and Testing)
- Call-Off Schedule 14A (Service Levels)
- Call-Off Schedule 14B (Service Levels and Balance Scorecard) – **Not Used**
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 16 (Benchmarking) – **Not Used**
- Call-Off Schedule 17 (MOD Terms) – **Not Used**
- Call-Off Schedule 18 (Background Checks)
- Call-Off Schedule 19 (Scottish Law) – **Not Used**
- Call-Off Schedule 20 (Call-Off Specification)
- Call-Off Schedule 21 (Northern Ireland Law) – **Not Used**
- Call-Off Schedule 23 (HMRC Terms) **Not Used**
- Call-Off Schedule 25 (Ethical Walls Agreement)
- Call-Off Schedule 26 (Secondment Agreement Template)

5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility) RM6263
7. 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.

No other Supplier terms are 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

None

FRAMEWORK SPECIAL TERMS

Special Term 1 - The following Core Terms shall be amended with deletions scored-through and insertions underlined as set out in the Framework Award Form:

Clause 6.3 (Record keeping and reporting)
A new Clause 8.8 (Restraint of Trade)
Clause 10.2.2 (Ending the Contract without a reason)
A new Clause 10.2.3
Clauses 10.6 (What happens if the Contract ends)
Clause 10.7.3 (Partially ending and suspending the Contract)
Clause 10.7.4
Clause 11.2 (How much you can be held responsible for)
Clause 14.4 (Data Protection)
New Clauses 23.7 and 23.8

Clause 25 (How to communicate about the contract)
Clause 34 (Resolving disputes)
A new Clause 36 (Counterparts)

CALL-OFF START DATE:	12 June 2025
CALL-OFF EXPIRY DATE:	11 June 2028
CALL-OFF INITIAL PERIOD:	3 Years
CALL-OFF OPTIONAL EXTENSION PERIOD:	Up to 25% of the initial term of the Call-Off Contract (6 months)
MINIMUM NOTICE PERIOD FOR EXTENSION(S):	1 Month
CALL-OFF CONTRACT VALUE:	£8,601,390 excluding VAT This is broken down as follows: - £5,734,260 excluding VAT for the initial period - £2,861,130 excluding VAT is a 50% contingency option for the initial period. This option requires further internal Buyer approvals (Cabinet Office digital and technology spend controls) in order to be exercised.
KEY SUB-CONTRACT PRICE:	N/A

CALL-OFF DELIVERABLES
Option B: See details in Call-Off Schedule 20 (Call-Off Specification)

BUYER's STANDARDS
From the Start Date of this Call-Off Contract, the Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards set out in Framework Schedule 1 (Specification).

The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract:

- Buyers Conduct Policy

MoJ
conduct-policy.pdf

- Buyers IT Security Policy

MoJ
it-security-policy.pdf

- Buyers Technical Guardrails (TG)
    - TG1: LTA - Languages Guardrail Feb 25
    - TG2: LTA-LAA Security Processes Feb 25
    - TG3: LTA-LAA Security Tooling Feb 25
    - TG4: LTA-Operational metrics guardrail Feb 25
    - TG5: LTA-Web analytics guardrail Feb 25

- Buyers Programme Test Strategy (TS)
    - TS1: Programme Test Strategy
    - TS2: Guiding Principles
    - TS3: Test Objectives and measurable success criteria
    - TS4: Approach to Testing
        - TS4.1: Test types and Tooling
        - TS4.2 Environments
        - TS4.3 Test Data
        - TS4.4 Testing Flow
        - TS4.5 Metrics
    - TS5: Striving for excellence

CYBER ESSENTIALS SCHEME

The Buyer requires the Supplier, in accordance with Joint Schedule 13 (CyberEssentials Scheme) to provide a Cyber Essentials Plus Certificate prior to commencing the provision of any Deliverables under this Call-Off Contract.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the CoreTerms, as amended by the Framework Award Form Special Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is £1,911,420 for the first 12 Months of the Contract.

CALL-OFF CHARGES

[REDACTED]

REIMBURSABLE EXPENSES

See Call-Off Schedule 5 (Pricing Details and Expenses Policy).

PAYMENT METHOD

[REDACTED]

BUYER'S INVOICE ADDRESS:

[REDACTED]

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]

BUYER'S ENVIRONMENTAL POLICY

N/A

BUYER'S SECURITY POLICY

Ministry of Justice IT Security Policy (attached).

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]

PROGRESS REPORT FREQUENCY

Monthly on a date set by the Buyers' Project Manager or as specified in the Statement of Work.

PROGRESS MEETING FREQUENCY

Monthly on a date set by the Buyers' Project Manager or as specified in the Statement of Work.

KEY STAFF

[REDACTED]

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION
The Supplier tender response (Schedule 4 tender including the Supplier rate card).

2 SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES

Professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);

Public liability and products insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and

Employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
The Supplier agrees, in providing the Deliverables andperforming its obligations under the Call-Off Contract, that it will comply with the socialvalue commitments in Call-Off Schedule 4 (Call-Off Tender).

STATEMENT OF WORKS
During the Call-Off Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisionsdetailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[REDACTED]	Signature:	[REDACTED]
Name:	[REDACTED]	Name:	[REDACTED]
Role:	[REDACTED]	Role:	[REDACTED]
Date:	[REDACTED]	Date:	[REDACTED]

Appendix 1

The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex1 to the Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules).

Each executed Statement of Work shall be inserted into this Appendix 1 in chronology.

Annex 1 (Template Statement of Work)

[REDACTED]

ANNEX 1

Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

[TEMPLATE ANNEX 1 OF JOINT SCHEDULE 11 (PROCESSING DATA BELOW]

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority isthe Controller and the Supplier is the Processor of the following Personal Data: • ***[Insert** the scope of Personal Data for which the purposes and means ofthe Processing by the Supplier is determined by the Relevant Authority]* **The Supplier is Controller and the Relevant Authority is Processor** *The Parties acknowledge that for the purposes of the Data Protection Legislation,the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:* • ***[Insert** the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier]* **The Parties are Joint Controllers** *The Parties acknowledge that they are Joint Controllers for the purposes of theData Protection Legislation in respect of:* • ***[Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]* **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposesof the Data Protection Legislation in respect of:* • *Business contact details of Supplier Personnel for which the Supplier isthe 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,* • ***[Insert** the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and*

	purposes of its Processing the Personal Data on receipt e.g. where (1)

	the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for useby the Relevant Authority] ***[Guidance** where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]*
Duration of the Processing	*[Clearly set out the duration of the Processing including dates]*
Nature and purposesof the Processing	*[Please be as specific as possible, but make sure that you cover all intendedpurposes.* *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	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public,users of a particular website etc.]*
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	*[Describe how long the data will be retained for, how it be returned or destroyed]*

Call-Off Schedule 5 (Pricing Details and Expenses Policy)

[REDACTED]

Annex 1 (Expenses Policy)

[REDACTED]

Annex 2 (Day Rates)

[REDACTED]

Call-Off Schedule 20 (Call-Off Specification)

[REDACTED]

Call-Off Schedule 4 (Call Off Tender)

[REDACTED]

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

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

"Breach of Security"	the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

2. Complying with security requirements and updates to them

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

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables, it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the

Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 Development of the Security Management Plan

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 Amendment of the Security Management Plan

4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

a) emerging changes in Good Industry Practice;

b) any change or proposed change to the Deliverables and/or associated processes;

c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

a) suggested improvements to the effectiveness of the Security Management Plan;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in within 24 hours and in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

6. Data security

6.1 The Supplier will ensure that any system on which the Supplier holds any Government Data will be accredited as specific to the Buyer and will comply with:

- the government security policy framework and information assurance policy (see: https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework);
- guidance on risk management (see: https://www.ncsc.gov.uk/collection/risk-management-collection);
- guidance issued by the Centre for Protection of National Infrastructure on Risk Management and Accreditation of Information Systems (see: http://osgug.ucaiug.org/conformity/security/Shared%20Documents/Reference/UK%20-%20CPNI%20-%20Risk%20Management%20and%20Accreditation%20of%20IS.pdf); and
- the relevant government information assurance standard(s) (see: https://knowledgehub.group/documents/49300605/0/bps68723-0000-00-hmg-ia-standard-numbers-1-and-2-information-risk-management.pdf/645c3ec5-e187-8124-16e8-ab9d86540cbb?t=1605540161981).

6.2 Where the duration of a Call-Off Contract exceeds one (1) year, the Supplier will review the accreditation status at least once each year to assess whether material changes have occurred which could alter the original accreditation decision in relation to Government Data. If any changes have occurred then the Supplier agrees to promptly re-submit such system for re-accreditation

Call-Off Schedule 14A (Service Levels)

1. Definitions

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

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels
"Service Credit Cap"	has the meaning given to it in the Order Form;
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.
"Replacement Plan"	in the event that the Buyer requests a replacement of a delivery team member, the Buyer and the Supplier shall, within 2 working days of the request and acting in good faith, agree the timeframe within which the replacement delivery team member will be provided to the Buyer, this shall form the "Replacement Plan";

2. What happens if you don't meet the Service Levels

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(c) results in the corruption or loss of any Government Data; and/or

(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and

2.5.3 there is no change to the Service Credit Cap.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2. Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

[REDACTED]

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

"Exclusive Assets"	Supplier Assets used exclusively by the Supplier or a Key Subcontractor in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Exit Plan"	the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier or a Key Subcontractor in connection with the Deliverables but which are also used by the Supplier or Key Subcontractor for other purposes;
"Registers"	the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer

	receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2. Supplier must always be prepared for Contract exit and SOW exit

2.1 The Supplier shall within 30 days from the Call-Off Contract Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables' IPR asset management system which includes all Document and Source Code repositories.

("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Call-Off Contract Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of each SOW and this Contract.

3. Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence whether this is in relation to one or more SOWs or the Call-Off Contract (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for

those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer a Call-Off Contract and SOW Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable (this may require modification to SOW Exit Plan provisions to be updated and incorporated as part of the SOW;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) prior to each SOW and no less than every six (6) months throughout the Contract Period; and

(b) no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable, in the case of the Call-Off Contract and each SOW (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular

Service Levels or KPI, the Parties shall vary the relevant KPIs, Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-Contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the **"Transferring Contracts"**), in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 15 (Call-Off Contract Management)

1. Definitions

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

"Operational Board"	the board established in accordance with paragraph 4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Managers in regards to the Contract and it will be the Supplier's Contract

Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks;

5.2.2 the identification and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Call-Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Operational Board Title:	TBC
Frequency of Meetings:	TBC
Location of Meetings:	Remote or 10 South Colonnade
Attendees:	**Buyer** Attendees TBC **Supplier** Supplier attendees TBC
Agenda and required reports:	1. Minutes of last meeting (Buyer) 2. Deliverable's tracker (Supplier) 3. RAID Log (Supplier) 4. Service Levels and Performance (Buyer) 5. Statements of Work/Variation Form (if applicable, Buyer and Supplier) 6. Billing – Purchase Orders, Invoices, reconciliations, forecast spend

Call-Off Schedule 1 (Transparency Reports)

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

[REDACTED]

Joint Schedule 11 (Processing Data)

Definitions

1. 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

2. 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:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "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

3. 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.

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

5. 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) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

(a) 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;

(b) 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:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) 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:

(A) 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;

(B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

(C) 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

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) 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:

(i) 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;

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

(iii) 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

(iv) 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

(e) 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.

7. 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:

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

(b) receives a request to rectify, block or erase any Personal Data;

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

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

(e) 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

(f) becomes aware of a Personal Data Breach.

8. 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.

9. 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:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) 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;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) 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.

10. 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:

(a) the Controller determines that the Processing is not occasional;

(b) 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

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

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

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

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) 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

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

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

15. 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).

16. 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.

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.

[REDACTED]

[REDACTED]

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

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

2.3 The Authority and Supplier jointly acknowledge that additional personal data may be processed to deliver the contract services and where such data is identified this schedule will be amended to specify that personal data before such processing commences.

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: Basic personal data of Supplier staff processed by the Authority for the purposes of delivering this contract. **The Supplier is Controller and the Relevant Authority is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data: Basic personal data of Authority staff processed by the Supplier for the purposes of delivering this contract.

Duration of the Processing	For the duration of this contract and for any period after the end of the contract where records must be maintained for audit purposes or statutory compliance.

Nature and purposes of the Processing	For the effective delivery of the services specified in this contract, included but not limited to the provision of IT equipment and user accounts, completion or assurance of vetting requirements, provision of contact points and billing and payment.
Type of Personal Data	Basic personal data consisting of names and contact details for Authority and Supplier staff, and confirmation of vetting status for Supplier staff.
Categories of Data Subject	Employees of the Authority and Supplier
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	The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system. • National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning • NCSC guidance on secure sanitisation of storage media: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media • NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation • Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): https://www.pcisecuritystandards.org • DIN: https://din66399.eu/

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

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

2. Supplier's Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

2.3.1 identifying the emergence of relevant new and evolving technologies;

2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so

as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

1. Definitions

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

"Delay"	a) a delay in the Achievement of a Milestone by its Milestone Date; or b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	1an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
"Milestone Payment"	2a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	3has the meaning given to it in Paragraph 7.1;

2. Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan 180 days after the Call-Off Contract Start Date.

2.2 The draft Implementation Plan:

2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively for the whole Call-Off Contract and each Statement of Work issued under it for the supply of Deliverables and as the Buyer may otherwise require;

2.2.2 shall provide details on how the required Social Value commitments will be delivered through the Call-Off Contract; and

2.2.3 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

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

2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

2.5 The Supplier shall also provide as required or requested reports to the Buyer concerning activities and impacts arising from Social Value including in the Implementation Plan.

2.6 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

2.7 The Supplier shall, in relation to each SOW, incorporate within it all Implementation Plan and Testing requirements for the satisfactory completion of each Deliverable Item to be provided under that SOW.

3. Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

3.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

3.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

4. Security requirements before the Start Date

4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.

4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5. What to do if there is a Delay

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

6. Compensation for a Delay

6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;

6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

7. Implementation Plan

7.1 The Implementation Period will be a [six (6)] Month period for the Call-Off Contract and for the duration of each SOW.

7.2 During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer in each SOW. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.

7.3 In accordance with the Implementation Plan, the Supplier shall:

7.3.1 work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where

applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;

7.3.2 work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and

7.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.

7.5 In addition, the Supplier shall:

7.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract and each SOW;

7.5.3 produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

(a) the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

(b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

7.5.4 manage and report progress against the Implementation Plan both at a Call-Off Contract level (which shall include an update on costings) and SOW level;

7.5.5 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

7.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form and each SOW) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

7.5.7 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

Annex 1: Implementation Plan

A.1 The Supplier shall provide a:

(a) high level Implementation Plan for the Call-Off Contract as part of the Further Competition Procedure; and

(b) a detailed Implementation Plan for each SOW.

A.2 The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

Milestone	Deliverable Items	Duration	Milestone Date	Buyer Responsibilities	Milestone Payments	Delay Payments
[ ]	[ ]	[ ]	]	[ ]	[ ]	]

ilestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)

e purposes of Paragraph 9.1.2 the Delay Period Limit shall be **[insert number of days]**.

Part B - Testing

1. Definitions

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

"Component"	4any constituent parts of the Deliverables;
"Material Test Issue"	5a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	6a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	7the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Issue Management Log"	8a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;
"Test Issue Threshold"	9in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Reports"	10 the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	11 the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule;
"Test Strategy"	12 a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;
"Test Success Criteria"	13 in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule;

"Test Witness"	14 any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and
"Testing Procedures"	15 the applicable testing procedures and Test Success Criteria set out in this Schedule.

2. How testing should work

2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.

2.2 The Supplier shall not submit any Deliverable for Testing:

2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and

2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

3. Planning for testing

3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.

3.2 The final Test Strategy shall include:

3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;

3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;

3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;

3.2.4 the procedure to be followed to sign off each Test;

3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;

3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;

3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;

3.2.8 the technical environments required to support the Tests; and

3.2.9 the procedure for managing the configuration of the Test environments.

4. Preparing for Testing

4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.

4.2 Each Test Plan shall include as a minimum:

4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and

4.2.2 a detailed procedure for the Tests to be carried out.

4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

5. Passing Testing

5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. How Deliverables will be tested

6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).

6.2 Each Test Specification shall include as a minimum:

6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

6.2.2 a plan to make the resources available for Testing;

6.2.3 Test scripts;

6.2.4 Test pre-requisites and the mechanism for measuring them; and

6.2.5 expected Test results, including:

(a) a mechanism to be used to capture and record Test results; and

(b) a method to process the Test results to establish their content.

7. Performing the tests

7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.

7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.

7.4 The Buyer may raise and close Test Issues during the Test witnessing process.

7.5 The Supplier shall provide to the Buyer in relation to each Test:

7.5.1 a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and

7.5.2 the final Test Report within 5 Working Days of completion of Testing.

7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

7.6.1 an overview of the Testing conducted;

7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;

7.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

7.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in

each case grouped by Severity Level in accordance with Paragraph 8.1; and

7.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

7.7 When the Supplier has completed a Milestone, it shall submit any Deliverables relating to that Milestone for Testing.

7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.

7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

8. Discovering Problems

8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the
Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.

8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

9. Test witnessing

9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and

requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

9.3.1 shall actively review the Test documentation;

9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

9.3.3 shall not be involved in the execution of any Test;

9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;

9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10. Auditing the quality of the test

10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.

10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.

10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.

10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.

10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction

Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

11. Outcome of the testing

11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:

11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;

11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require
the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:

11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.

11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).

11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.

11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.

11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.

11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer's report pursuant to Paragraph 10.5); and

11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

12. Risk

12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:

12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or

12.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:

2.1.1 causes a Component to become unusable;

2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

3.1 This is an error which:

3.1.1 causes a Component to become unusable;

3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;

but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

5. Severity 5 Error

5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

Annex 2: Satisfaction Certificate

To: [insert name of Supplier]

From: [insert name of Buyer]

[insert Date dd/mm/yyyy]

Dear Sirs,

Satisfaction Certificate

Deliverable/Milestone(s): [Insert relevant description of the agreed Deliverables/Milestones].

We refer to the agreement (**"Call-Off Contract"**) [insert Call-Off Contract reference number and any applicable SOW reference] relating to the provision of the [insert description of the Deliverables] between the [*insert Buyer name*] (**"Buyer"**) and [*insert Supplier name*] (**"Supplier"**) dated [*insert Call-Off Start Date dd/mm/yyyy*].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

[insert Name]

[insert Position]

acting on behalf of [insert name of Buyer]

and

[SUPPLIER]

ETHICAL WALLS AGREEMENT

DRAFTING INSTRUCTIONS: ETHICAL WALLS AGREEMENT	
[DELETE THIS INSTRUCTION TABLE BEFORE CIRCULATING]	This standard document has been written from the perspective of the
Applicability	Buyer. Its intended use is as an ethical walls agreement between a Government Department and an incumbent company which intends to submit a tender for a Further Competition Procedure for the Deliverables in question. It will need amending if one of the parties is an individual, partnership or a limited liability partnership (LLP).
Term	Clause 10.1 should be completed with the appropriate period of time being at least as long as the Further Competition Procedure will take to be completed.
Context	This document is a template and may require amendment to suit the circumstances of the transaction you are working on. Please ensure that this document is used in the correct context and amended to reflect that context where necessary. If you are using it as part of a suite of documents make sure that you have amended it to reflect the deal you are working on.
Required action	Highlighted text in this document requires action as follows: a) Optional provision to be deleted if not required or amended to reflect the circumstances and b) Details to be inserted.

Version history:

Document last reviewed by GLD on 1 March 2020

This Agreement is dated [ ] 20[ ]

Between

(1) **[INSERT NAME OF BUYER]** (the **"Buyer"**) [acting on behalf of the Crown] of [insert Buyer's address] ; and

(2) **[NAME OF SUPPLIER]** a [company]/[limited liability partnership] registered in England and Wales under registered number [insert registered number] whose registered office is at [insert Supplier's registered address] (the **"Supplier"**).

together the "**Parties**" and each a "**Party**".

BACKGROUND

A. The Buyer is obliged to ensure transparency, fairness, non-discrimination and equal treatment in relation to its procurement process pursuant to the Public Contracts Regulations 2015 (as amended) (the **PCR)**. The purpose of this document ("Agreement") is to define the protocols to be followed to prevent, identify and remedy any conflict of interest (whether actual, potential or perceived) in the context of the Further Competition Procedure.

B. The Buyer is conducting a Further Procurement Procedure for the supply of Digital Outcomes and Specialists 5 Deliverables under a Call-Off Contract (the **"Purpose"**).

C. The Buyer has an obligation to deal with conflicts of interest as set out in Regulation 24 (1) of the PCR. The concept of conflict of interest is wide. In the PCR it is described as covering at least *"any situation where relevant staff members have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure"* (Regulation 24(2)). *"Staff members"* refers to staff members of the Buyer or of a procurement service provider acting on behalf of the Buyer who are involved in the conduct of the procurement procedure or may influence the outcome of that procedure. *"Procurement service provider"* refers to a public or private body which offers ancillary purchasing activities on the market.

D. Pursuant to Regulation 41 of the PCR, the Buyer is under an obligation to ensure that competition is not distorted by the participation of any Framework Contract supplier acting as a bidder in a further competition procedure. Accordingly, the Buyer has identified that a potential distortion of competition could arise as a consequence of a bidder wishing to submit a Tender for this Further Competition Procedure, where it has also performed services for the Buyer under existing contractual arrangements or as a subcontractor under those same arrangements.

E. The Parties wish to enter into this Agreement to ensure that a set of management processes, barriers and disciplines are put in place to ensure that conflicts of interest do not arise, and that the Supplier does not obtain an unfair competitive advantage over Other Bidders.

IT IS AGREED:

1 DEFINITIONS AND INTERPRETATION

1.1 The following words and expressions shall have the following meanings in this agreement and its recitals:

"**Affiliate**" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

"**Agreement**" means this ethical walls agreement duly executed by the Parties;

"**Bid Team**" means any Supplier, Affiliate, connected to the preparation of an FCP Response;

"**Central Government Body**" means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:

a) Government Department;
b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);
c) Non-Ministerial Department; or

d) Executive Agency.

"**Conflicted Personnel**" means any Supplier, Affiliate, staff or agents of the Supplier or an Affiliate who, because of the Supplier's relationship with the Buyer under any Contract have or have had access to information which creates or may create a conflict of interest;

"**Contract**" means the [contract for [ ] dated [ ] between the Buyer and the Supplier and/or an Affiliate;

"**Control**" means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and "**Controls**" and "**Controlled**" shall be interpreted accordingly;

"**Effective Date**" means the date of this Agreement as set out above;

"**Further Competition Procedure**" or "**FCP**" means an invitation to submit tenders issued by the Buyer as part of an FCP Process;

"**FCP Process"** means, with regard to the Purpose, the relevant procedure provided for in Framework Schedule 7 (Call-Off Award Procedure) of RM1043.7 Framework Contract which the Buyer has elected to use to select a contractor, together with all relevant information, correspondence and/or documents issued by the Buyer as part of that procurement exercise, all information, correspondence and/or documents issued by the bidders in response together with any resulting contract;

"FCP Response" means the tender submitted or to be submitted by the Supplier or an Affiliate [(or, where relevant, by an Other Bidder)] in response to an FCP;

"Other Affiliate" any person who is a subsidiary, subsidiary undertaking or holding company of any Other Bidder;

"Other Bidder" means any other bidder or potential bidder that is not the Supplier or any Affiliate that has or is taking part in the FCP Process;

"Parties" means the Buyer and the Supplier;

"**Professional Advisor**" means a supplier, subcontractor, advisor or consultant engaged by the Supplier under the auspices of compiling its FCP Response;

"**Purpose**" has the meaning given to it in recital B to this Agreement;

"**Representative"** refers to a person's officers, directors, employees, advisers and agents and, where the context admits, providers or potential providers of finance to the Supplier or any Affiliate in connection with the FCP Process and the representatives of such providers or potential providers of finance; and

"**Third Party**" means any person who is not a Party and includes Other Affiliates and Other Bidders.

1.2 Reference to the disclosure of information includes any communication or making available information and includes both direct and indirect disclosure.

1.3 Reference to the disclosure of information, or provision of access, by or to the Buyer or the Supplier includes disclosure, or provision of access, by or to the representatives of the Buyer or Representatives of the Supplier (as the case may be).

1.4 Reference to persons includes legal and natural persons.

1.5 Reference to any enactment is to that enactment as amended, supplemented, re-enacted or replaced from time to time.

1.6 Reference to clauses and recitals is to clauses of and recitals to this Agreement.

1.7 Reference to any gender includes any other.

1.8 Reference to writing includes email.

1.9 The terms "associate", "holding company", "subsidiary", "subsidiary undertaking" and "wholly owned subsidiary" have the meanings attributed to them in the Companies Act 2006, except that for the purposes of section 1159(1)(a) of that Act, the words 'holds a majority of the voting rights' shall be changed to 'holds 30% or more of the voting rights', and other expressions shall be construed accordingly.

1.10 The words "include" and "including" are to be construed without limitation.

1.11 The singular includes the plural and vice versa.

1.12 The headings contained in this Agreement shall not affect its construction or interpretation.

2 ETHICAL WALLS

2.1 In consideration of the sum of £1 payable by the Buyer to the Supplier, receipt of which is hereby acknowledged, the Supplier:

2.1.1 shall take all appropriate steps to ensure that neither the Supplier nor its Affiliates and/or Representatives are in a position where, in the reasonable opinion of the Buyer, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier or its Affiliates or Representatives and the duties owed to the Buyer under the Contract or pursuant to an fair and transparent FCP Process;

2.1.2 acknowledges and agrees that a conflict of interest may arise in situations where the Supplier or an Affiliate intends to take part in the FCP Process and, because of the Supplier's relationship with the Buyer under any Contract, the Supplier, its Affiliates and/or Representatives have or have had access to information which could provide the Supplier and/or its Affiliates with an advantage and render unfair an otherwise genuine and fair competitive FCP Process; and

2.1.3 where there is or is likely to be a conflict of interest or the perception of a conflict of interest of any kind in relation to the FCP Process, shall comply with Clause 2.2.

2.2 The Supplier shall:

2.2.1 Not assign any of the Conflicted Personnel to the Bid Team at any time;

2.2.2 Provide to the Buyer a complete and up to date list of the Conflicted Personnel and the Bid Team and reissue such list upon any change to it;

2.2.3 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates results in information of any kind or in any format and however so stored:

(a) about the Contract, its performance, operation and all matters connected or ancillary to it becoming available to the Bid Team; and/or

(b) which would or could in the opinion of the Buyer confer an unfair advantage on the Supplier in relation to its participation in the FCP Process becoming available to the Bid Team;

2.2.4 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates and in particular the Bid Team results in information of any kind or in any format and however so stored about the FCP Process, its operation and all matters connected or ancillary to it becoming available to the Conflicted Personnel;

2.2.5 Ensure that confidentiality agreements which flow down the Supplier's obligations in this Agreement are entered into as necessary between the Buyer and the Supplier, its Affiliates, its staff, agents, any Conflicted Personnel, and between any other parties necessary in a form to be prescribed by the Buyer;

2.2.6 physically separate the Conflicted Personnel and the Bid Team, either in separate buildings or in areas with restricted access;

2.2.7 provide regular training to its staff, agents and its Affiliates to ensure it is complying with this Agreement;

2.2.8 monitor Conflicted Personnel movements within restricted areas (both physical and electronic online areas) to ensure it is complying with this Agreement ensure adherence to the ethical wall arrangements;

2.2.9 ensure that the Conflicted Personnel and the Bid Team are line managed and report independently of each other; and

2.2.10 comply with any other action as the Buyer, acting reasonably, may direct.

2.3 In addition to the obligations set out in Clause 2.1.1 and 2.1.3, the Supplier shall:

2.3.1 notify the Buyer immediately of all perceived, potential and/or actual conflicts of interest that arise;

2.3.2 submit in writing to the Buyer full details of the nature of the conflict including (without limitation) full details of the risk assessments undertaken, the impact or potential impact of the conflict, the measures and arrangements that have

been established and/or are due to be established to eliminate the conflict and the Supplier's plans to prevent future conflicts of interests from arising; and

2.3.3 seek the Buyer's approval thereto,

which the Buyer shall have the right to grant, grant conditionally or deny (if the Buyer denies its approval the Supplier shall repeat the process set out in clause 2.3 until such time as the Buyer grants approval or the Supplier withdraws from the FCP Process).

2.4 Any breach of Clause 2.1, Clause 2.2 or Clause 2.3 shall entitle the Buyer to exclude the Supplier or any Affiliate or Representative from the FCP Process, and the Buyer may, in addition to the right to exclude, take such other steps as it deems necessary where, in the reasonable opinion of the Buyer there has been a breach of Clause 2.1, Clause 2.2 or Clause 2.3.

2.5 The Supplier will provide, on demand, any and all information in relation to its adherence with its obligations set out under Clauses 2.1 and 2.2 as reasonably requested by the Buyer.

2.6 The Buyer reserves the right to require the Supplier to demonstrate the measures put in place by the Supplier under Clauses 2.1.3 and 2.2.

2.7 The Supplier acknowledges that any provision of information or demonstration of measures, in accordance with Clauses 2.5 and 2.6, does not constitute acceptance by the Buyer of the adequacy of such measures and does not discharge the Supplier of its obligations or liability under this Agreement.

2.8 The actions of the Buyer pursuant to Clause 2.4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Buyer.

2.9 In no event shall the Buyer be liable for any bid costs incurred by:

2.9.1 the Supplier or any Affiliate or Representative; or

2.9.2 any Other Bidder, Other Affiliate or Other Representative,

as a result of any breach by the Supplier, Affiliate or Representative of this Agreement, including, without limitation, where the Supplier or any Affiliate or Representative, or

any Other Bidder, Other Affiliate or Other Representative are excluded from the FCP Process.

2.10 The Supplier acknowledges and agrees that:

2.10.1 neither damages nor specific performance are adequate remedies in the event of its breach of the obligations in Clause 2; and

2.10.2 in the event of such breach by the Supplier of any of its obligations in Clause 2 which cannot be effectively remedied the Buyer shall have the right to terminate this Agreement and the Supplier's participation in the FCP Process.

3 SOLE RESPONSIBILITY

3.1 It is the sole responsibility of the Supplier to comply with the terms of this Agreement. No approval by the Buyer of any procedures, agreements or arrangements provided by the Supplier or any Affiliate or Representative to the Buyer shall discharge the Supplier's obligations.

4 WAIVER AND INVALIDITY

4.1 No failure or delay by any Party in exercising any right, power or privilege under this Agreement or by law shall constitute a waiver of that or any other right, power or privilege, nor shall it restrict the further exercise of that or any other right, power or privilege. No single or partial exercise of such right, power or privilege shall prevent or restrict the further exercise of that or any other right, power or privilege.

4.2 If any provision of this Agreement is prohibited or unenforceable in any jurisdiction in relation to any Party, such prohibition or unenforceability will not invalidate the remaining provisions of this Agreement or affect the validity or enforceability of the provisions of this Agreement in relation to any other Party or any other jurisdiction.

5 ASSIGNMENT AND NOVATION

5.1 Subject to Clause 5.2 the Parties shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Buyer.

5.2 The Buyer may assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:

5.2.1 any Central Government Body; or

5.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority; and

5.2.3 the Supplier shall, at the Buyer's request, enter into a novation agreement in such form as the Buyer reasonably specify in order to enable the Buyer to exercise its rights pursuant to this Clause 5.

5.3 A change in the legal status of the Buyer such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Buyer.

6 CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

6.1 A person who is not a Party to this Agreement has no right under the Contract (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any term of this Agreement but this does not affect any right remedy of any person which exists or is available otherwise than pursuant to that Act.

7 TRANSPARENCY

7.1 The Parties acknowledge and agree that the Buyer is under a legal duty pursuant to the PCR to run transparent and fair procurement processes. Accordingly, the Buyer may disclose the contents of this Agreement to potential bidders in the FCP Process, for the purposes of transparency and in order to evidence that a fair procurement process has been followed.

8 NOTICES

8.1 Any notices sent under this Agreement must be in writing.

8.2 The following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

Manner of Delivery	**Deemed time of service**	**Proof of service**
Email	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an email to the correct email address without any error message.
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt.
Prepaid, Royal Mail Signed For™ 1st Class or other prepaid, next working day service providing proof of delivery.	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

8.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:

	Supplier	**Buyer**
Contact		

Address

Email		

8.4 This Clause 8 does not apply to the service of any proceedings or other documents in any legal action or other method of dispute resolution.

9 WAIVER AND CUMULATIVE REMEDIES

9.1 The rights and remedies under this Agreement may be waived only by notice and in a manner that expressly states that a waiver is intended and what is waived. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

9.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

10 TERM

10.1 Each Party's obligations under this Agreement shall continue in full force and effect for a period of [ ] years from the Effective Date.

11 GOVERNING LAW AND JURISDICTION

11.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.

11.2 The Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

Signed by the Buyer Name:

Signature:

Position in

Buyer:

Signed by the Supplier

Name:

Signatu

re:

Position in Supplier:

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality

PROTECT

RM6263
Secondment Agreement

Crown Commercial Service

1

SECONDMENTAGREEMENT

Introduction

1. Secondments, in or out of the Civil Service, are a valuable way to exchange knowledge and skills with other sectors and, as such, departments are actively encouraged to use them.

   A secondment is a move between a Civil Service department and an external organisation, such as the wider public, voluntary or private sector, for an agreed time period.

2. Secondments are either:

   Outward; when a Civil Service employee moves temporarily to work in an external organisation outside of the Civil Service, but remains employed by the Civil Service.

   Inward; when an individual from outside of the Civil Service moves temporarily to work for a Civil Service department but remains employed by their external organisation.

The benefits a secondment can bring

3. Secondments are a key element of the Civil Service development offer and talent development strategy. They provide opportunities to:

   - develop specific skills required for organisational performance that cannot be developed within the Civil Service
   - develop talent via recognised programmes
   - build a broader understanding of departmental delivery chains and relationships with strategic partners.

4. Secondments:

   - bring new skills back into the business
   - build capability through skills transfer between the Civil Service and external organisations
   - offer development opportunities to employees
   - increase awareness of customers and the impacts departments have on them
   - support employers in other sectors to build their capability.

What to know before you start

5. **The Civil Service Management Code (section 10.3)** gives particular information around:

   - Conduct and discipline
   - Pensions arrangements
   - Injury Benefits
   - Recruiting to inward secondments
   - Pre-appointment checks for inward secondments

   These are referenced in this guidance at appropriate points. Details of further Civil Service guidance which may be useful when considering a secondment can be found at Annex 1.

Discussing secondment opportunities

6. Discussing a potential secondment with an external organisation will require an element of negotiation for either an inward or an outward placing. To get the best outcome it is advisable to:

    - start discussions as early as possible; involving departmental HR, finance, and where necessary legal colleagues from the outset

    - be clear about Civil Service rules or requirements: e.g. the Civil Service Commission's Recruitment Principles allow inward secondments of up to two years without the need for fair and open competition

    - ensure that the individual being seconded understands and is a part of any discussions at the appropriate stage

    - be flexible wherever possible; but also be aware of the wider aims of the secondment and keep the business benefits at the forefront of discussions.

Outward secondments

Glossary of terms

Employee - Current civil servant undertaking a secondment in an external organisation.

Host organisation - An external organisation that is not part of the Civil Service.

Home department - Civil Service department where the employee is permanently employed.

Requests for secondments

7. When an employee considers a secondment would be beneficial to their development they should talk this through with their manager. Completing the business case template at Annex 2 is a good way to help both parties decide if the opportunity would be a good one for the employee and provide benefits to the business.

Eligibility

8. To be eligible for a secondment an employee must:

    - have been recruited in line with the Civil Service Commission's Recruitment principles (appointment on merit through fair and open competition)
    - be in a position to clearly benefit from development outside of the Civil Service
    - have successfully completed their probationary period
    - demonstrate acceptable performance and attendance levels
    - not have an immigration visa restriction which specifies a particular place of work.

9. If an eligible employee is on a fixed term contract consider the decision alongside the business benefit in relation to:

    - fixed term employees are usually recruited to undertake a specific piece of work
    - the secondment can only be agreed for the remaining duration of the fixed term contract or less
    - there may be limited opportunities for the employee to bring skills back to the department.

Business benefits

10. If an employee meets the eligibility criteria, managers will need to consider the business benefits that will be gained by the department and the wider Civil Service as a result of the secondment.

Decision making

11. If it is agreed the secondment is a good opportunity, a consideration may be how to fill the role left by the employee going on secondment. There may be occasions when their specific role should be retained for them, for example where they have gone on secondment to bring back specific skills to the business; or their post can be filled

permanently depending on the type of post and length of secondment. The following options can also be considered:

- offering the role to an employee on a development programme
- asking for an exchange with the host organisation
- advertising the role as a loan.

[DN: Department to insert link to approval process for vacancy filling].

Communicating decisions

12. Managers should communicate the decision to the employee by providing clear reasons and rationale, particularly where the secondment is refused. If refused, managers should consider other ways in which the employee could be further developed.

Agreements for secondments

13. The Civil Service Management Code states that the terms of the secondment are for negotiation between the home department, the host organisation and the employee.

14. A written agreement which is understood by all parties should be in place before a secondment begins. This is normally, but not exclusively, written by the home department with input by the host organisation.

15. A template for an outward secondment agreement is available at Appendix 1.

The agreement should cover

16. **Duration** This should be appropriate to the nature of the opportunity and not exceed two years unless there is a specific business justification for doing so. Outward secondments are to develop new skills for the Civil Service and the duration should reflect this. The agreement should include an **end date**.

Notice Periods should be agreed to cover circumstances where either the home department or the host organisation needs to terminate the agreement.

Pay The usual arrangement is for the employee to continue to be on the payroll and receive the pay awards of their home department with the external organisation reimbursing the salary costs. Moving employees to the payroll of the external organisation is not recommended as there are implications regarding Civil Service Pension Schemes contributions and reckonable service.

Employees may not necessarily continue to be entitled to non contractual allowances they are in receipt of in the home department.

Reimbursement There can be variations in how much salary is reimbursed. There are occasionally circumstances where the home department may agree not to be reimbursed, or may be partially reimbursed, for example where the secondment is very short or where there is a significant business benefit which offsets the cost. This will need to be agreed by **[DN departments to insert relevant approvals route].**

As the employee remains on their home department's payroll during a secondment, VAT is applied to the salary as the host organisation is considered to be purchasing a service from the home department.

Pensions Regardless of whether the employee will remain on their department's payroll during the secondment the employee must be given a written statement of the effect upon their pension arrangements. Managers will need to refer to their departmental pension's administrator regarding this.

Automatic enrolment Duties should be included within the secondment agreement. As employees retain the terms and conditions of their home department and remain on their payroll, it is the home department that is responsible for automatically enrolling the worker under legislation.

Injury benefits If the employee remains in the pension scheme of their department they must receive injury benefit cover from the department. In other cases, the receiving organisation must provide the cover. Departmental pension's administrators will be able to provide advice where there is any doubt about liability. A written statement must be given to the employee explaining who is providing the injury benefit. It is advisable to do this within the secondment agreement.

Terms and Conditions The secondment agreement will specify any changes to contractual terms but the employee will normally remain on those of their home department.

Policies There should be a clear understanding of the policies the employee is working under during the secondment. A practical approach may be to use the host organisation's policies for day to day management activities but where policies link to payroll mechanisms it may be better to use those of the home department.

Conduct and Business Appointment Rules A civil servant on outward secondment remains subject to the Civil Service Management Code and the existing rules of their home department. The Business Appointment Rules continue to apply. During the secondment, the employee must also behave as if they were members of the host organisation in following its policies and directives.

Return arrangements The secondment agreement should outline what post the employee is eligible to return to at the end of the secondment period; the minimum commitment should be that a department will accept the employee back at their previous grade and location where possible. If there is no post available or the home department no longer occupies the previous location, the employee will be declared surplus.

Duty of care. The agreement should be clear about the responsibility to protect the employee from reasonably foreseeable risk or harm which might occur as a result of their work. The under-pinning principle is that a home department will always retain responsibility for the duty of care but that it can choose to discharge this responsibility by asking the host organisation to take responsibility for some or all aspects.

At the start of the secondment

17. Once the secondment is agreed, the practical steps to facilitate the transfer will need to be undertaken. A line manager checklist is available at Annex 3.

    A **home** manager should:

    - confirm the employee has been recorded as going on secondment
    - ensure that keep in touch arrangements have been agreed.

During the secondment

Keep in Touch

18. Keep in touch activities need to be tailored to suit all parties. Key things to consider are:

    - method, e.g. tele-kit, video conference, face to face, telephone
    - departmental information required such as newsletters or vacancy bulletins
    - frequency e.g. weekly, monthly
    - other information required by the host line manager, which will depend on the payroll and management arrangements in place.

    The home line manager has overall responsibility for maintaining the programme of keeping in touch and ensuring a smooth return process. They should review the employee's development goals and ensure they have an effective development plan.

    - They are also responsible for updating the employee about key developments such as:

      -any promotion opportunities

      -any restructuring taking place within the home department

      -early release schemes they may be eligible to apply for whilst on secondment.

    - **The employee** is responsible for ensuring the agreed keep in touch arrangements are followed, actively informing both managers of any changes or developments in their home department and the timescales for returning at the end of the secondment.

    - **The host line manager** is responsible for engaging with and supporting the keep in touch process.

Managing the employee whilst on secondment

19. As the employee remains on their home departmental payroll, their home line manager will need to ensure that they are taking all necessary action linked to pay. This includes but is not limited to: performance management, annual leave and sick pay.

20. All the actions taken for an employee on secondment should be recorded to ensure they are not treated differently from other employees managed under those policies.

21. It can be complex for a host line manager to manage individuals on secondment using unfamiliar policies, processes and entitlements. Home line managers should be as helpful as possible in interpreting departmental policies and supporting with any issues that arise.

Ending early

22. Secondments will usually come to an end at the pre-agreed end date but either the home department or host organisation can terminate the secondment by giving the agreed notice.

23. A secondment may need to end because:

- the employee accepts a new permanent role
- the home department encounters exceptional resourcing issues and requests that the employee return early (this would only be due to an urgent business need)
- significant business change in either the home department or host organisation, for example a TUPE or Machinery of Government change
- the secondment is not working successfully and discussion has not resolved the problem.

Towards the end of the secondment

24. As part of the keep in touch arrangement it is important to plan the employee's return to the home department.

    This should include a review of the benefits of the secondment and any discussion of how further benefit could be achieved in the time remaining. It is important to assess this against the benefits listed in the original business case, the objectives set for the employee and progress made.

    If it is confirmed that the secondment will end at the pre-agreed time the home department needs to start considering what post the employee will return to. The department will also need to consider how best to use the development the employee has gained from the secondment.

Extending the secondment

25. In exceptional circumstances the host organisation may wish to extend the secondment. They can make this request but the home department will need to agree. This decision should be based on the original purpose of the secondment and an assessment of the continued benefits to all parties. A secondment's purpose is to bring new skills into the Civil Service; those which are extended may not deliver this. The outcome of the extension request should be recorded formally so that all parties are aware of the outcome.

At the end of the secondment

26. It is essential that the employee and home line manager regularly communicate and plan well in advance the practical arrangements that need to be made to facilitate an

effective return. This will include any steps required to induct the employee back into the organisation and any payroll amendments which may be required.

Both the home department and the host organisation should take part in a review meeting to hand over fully, following the secondment.

Employees should be kept fully up-to-date with any organisational changes which may alter the return arrangements. In the event that it is not possible to accommodate the employee as planned, the employee should be notified as soon as possible, and managed in line with the home department's surplus policies.

Evaluation and using new skills

27. When an employee returns to the department they should meet with their home manager to:

- review the outcomes of the keep in touch meeting which took place towards the end of the secondment
- discuss and evaluate the benefits gained from the secondment compared with the original objectives and agree next steps to build on the experience. It may also be useful to have a follow up evaluation once the employee has been back in post for a number of months.
- find ways to share their learning in their work environment.

Further help

28. The Frequently Asked Questions provide further detailed advice in response to questions that employees or managers may ask when considering a secondment opportunity.

Inward Secondments

Glossary of terms

Individual Current employee of an external organisation, undertaking a secondment in a Civil Service department; they will not be a current civil servant.

Home organisation External organisation where the individual is permanently employed

Host department Civil Service department where the individual is undertaking the secondment.

Using secondments to fill a role

29. As secondments are classed as external recruitment they are subject to the requirements of the Civil Service Commission's Recruitment Principles. Secondments into the Civil Service are also covered by the recruitment freeze. As such use of them will require discussion with senior management and be subject to existing departmental processes to gain approval to recruit externally. The benefits to the department and the wider Civil Service will need to be made clear as part of this process.

30. Inward secondments must be conducted in line with the Civil Service Commission's Recruitment Principles. To facilitate movement between the Civil Service and other employers the Commission allows **secondments of up to two years without the need for recruitment via fair and open competition based on merit**.

31. Numbers of inward secondments need to be included in departmental annual reports to the Civil Service Commission.

Advertising

32. Secondment opportunities could be advertised on CS Jobs, through professional networks or to communities using that profession's website. If advertised on CS Jobs this would be classed as appointment on merit through fair and open competition and the limit of two years would not apply. However, as the aim of a secondment is to develop skills within the Civil Service, longer periods should not normally be required.

Direct placement

33. Secondments may also be filled by identifying a suitable individual, where:

    - a department approaches an individual, employed by an external organisation, with very specialised skills to carry out particular work, and the individual's organisation agrees to a secondment
    - pre-existing 'exchange' arrangements exist between Civil Service departments and external organisations or professions as part of a recognised scheme
    - an individual has a particular development need or interest and there is an opportunity which is suitable, available and of business benefit to the department.

34. It is important that all activity undertaken to fill a role using a secondment is in line with equality legislation.

Applications for secondments

35. When considering a secondment application, the potential host manager should assess it in line with the requirements of the role. They should make clear to the individual the duration, salary, terms of secondment, and the need for agreement from the home organisation.

36. They will also need to make clear to the individual that the role is offered on a secondment basis and is not an offer of permanent employment.

Pre-appointment checks

37. Managers will need to ensure that personnel security risks are effectively managed by applying controls and checks relevant to the specific secondment post. The Civil Service Nationality Rules will not apply where the individual remains the employee of an external organisation. As the individual is working within the Civil Service they will require all other pre-appointment checks in the same way as a permanent new starter. This will also include ensuring that the individual does not have any visa restrictions that limit the secondment. It is helpful to make individuals aware of the pre-appointment checks process, any timescales involved, and additional restrictions that would otherwise apply if employed directly by the Civil Service.

    Annex 1 lists guidance to be aware of. These checks should be conducted in line with departmental recruitment guidance **[DN: Department to insert links].**

Secondment agreements

38. The Civil Service Management Code states that the terms of a secondment are a matter for negotiation between the home organisation, the host department and the individual.

    A secondment should always be under-pinned by a written agreement between all parties. A template for an inward secondment agreement is available at Appendix 2.

    During an inward secondment the individual will be carrying out work for the Civil Service department whilst remaining employed by their home organisation. The home organisation's agreement would normally be used. As long as the department's interests are represented the template used should not be a barrier. The department can suggest the use of the template at Appendix 2 if the home organisation agrees.

Checking the details of an agreement

39. Consider:

    Duration and end date To facilitate movement between the Civil Service and other employers the Commission allows secondments of up to two years without the need for recruitment via fair and open competition based on merit. Any proposal for a longer secondment at the outset, or to extend the appointment beyond two years requires the approval of the Commission. Timescales in agreements should reflect this.

Notice periods should be agreed to cover circumstances where either the home organisation or the host department needs to terminate the agreement.

Pay The usual arrangement is for the individual to continue to be on the payroll of the home organisation and be covered by their pay arrangements, with the host department reimbursing salary costs. Departments should not normally agree to reimburse variable pay such as bonuses.

Reimbursement VAT is payable by the host department as they will need to use an invoice to pay the home organisation for the individual's costs; this is because during a secondment the individual remains on their home organisation's payroll.

Automatic enrolment duties should be included within the secondment agreement. As the individual will retain the terms and conditions of their employer and remain on their payroll, it is the home organisation that is responsible for automatically enrolling the worker under legislation.

Injury benefits Arrangements for injury benefit cover must be agreed before any inward secondment commences and given to the secondee in writing, explaining who provides the benefit and what it is comprised of. If the individual remains in the pension scheme of their home organisation they should receive injury benefit cover from them. In other cases, the host must provide the cover. Departmental pension's administrators will be able to provide advice where there is any doubt about liability.

Terms and Conditions The secondment agreement will specify any temporary changes to contractual terms but the individual will normally remain on those of their home organisation.

Policies There should be a clear understanding of which policies the individual is working under during the secondment. Where policies link to pay systems it may be better to use those of their home organisation whilst following those of the host department for areas linked to day to day management activity.

Conduct Individuals seconded in to the Civil Service must be made aware that they will be subject to the Official Secrets Acts and are also required to observe the Civil Service and departmental rules on conduct, confidentiality and security. They should ensure that there is no conflict of interest that will cause embarrassment either to their home organisation or their host department. These may be in addition to rules that are applicable to them in their home organisation.

Duty of care The agreement should be clear about the responsibility to protect the individual from reasonably foreseeable risk or harm which might occur as a result of their work. The under-pinning principle is that a home organisation will always retain responsibility for the duty of care but that it can choose to discharge this responsibility by asking the host department to take responsibility for some or all aspects.

At the start of the secondment

40. Once the secondment is agreed, the practical steps to facilitate the transfer will need to be undertaken.

    A **host** manager should be aware of:

- any reasonable adjustments required and ensure these are in place
- keep in touch arrangements and responsibilities that have been agreed
- arrangements for paying the individual, including expenses
- the arrangements for managing the individual and whose policies they are working under
- the external organisation's policies that relate to pay such as performance management, annual leave, attendance management.

During the secondment

Keep in touch

41. Keeping in touch during the secondment is the responsibility of all the parties involved:

    - **The individual** is responsible for ensuring the agreed keep in touch arrangements are followed, actively informing both managers of any changes and the timescales for returning at the end of the secondment.
    - **The home line manager** has overall responsibility for maintaining the keep in touch programme and ensuring a smooth return process. They will need to liaise with their employee and provide the host line manager with information needed to manage the individual.
    - **The host line manager** is responsible for engaging with, and supporting, the keep in touch process and supplying information required by the home organisation.

Managing the employee

42. During the secondment the host line manager is responsible for the day to day management of the individual and should maintain accurate records which can be shared with the home organisation as necessary.

    As the individual remains on their home organisation's payroll, the policies linked to pay will need to be adhered to and any required action taken; these will include performance management, annual leave and attendance management.

    Both managers should discuss and agree what the requirements are in terms of record keeping and paperwork.

    It can be complex managing individuals on secondment where some of the policies used are those of the home organisation and as a result are unfamiliar to the host line manager. In order to ensure the process runs smoothly any issues that arise which are covered by the home organisation's policies, processes and entitlements should be discussed with the home manager as part of the keep in touch process.

Ending a secondment early

43. Secondments will usually come to an end at the pre-agreed end date. Either the host department or the home organisation can terminate the secondment early by giving the agreed notice period.

44. A secondment may need to end early because:

- the individual accepts a new permanent job role
- the individual returns to the home organisation due an urgent business requirement
- the secondment is not working successfully and discussion has not resolved the problem.

Towards the end of the secondment

45. Towards the end of the secondment a review of the benefits of the secondment, and any discussion of how further benefit could be achieved in the time remaining, should be undertaken. This should involve the home organisation as this will support the evaluation process and build links for future opportunities.

Extending the secondment

46. As inward secondments are used to transfer skills and facilitate movement between the Civil Service and other employers, the Civil Service Commission allows **secondments of up to two years without the need for recruitment via fair and open competition based on merit**.

    Any proposal for a longer secondment at the outset, or to extend the appointment beyond two years requires the approval of the Commission. Additional information is available from the Commission's website.

At the end of the secondment

47. Activity undertaken at the end of the secondment should include:

- Performing a review of the secondment and the skills and benefits it has brought for: the host department, the individual, the home organisation and the wider Civil Service. This will be key for informing future secondment activity.

- Considering keeping in contact with the individual as a way to build networks outside of the Civil Service which could lead to similar arrangements in the future.

Further help

48. The Frequently Asked Questions provide further detailed advice in response to questions that employees or managers may ask when considering a secondment opportunity.

Annex 1 – Civil Service guidance and rules to consider

Section 10.3 of the Civil Service Management Code sets out rules concerning:

- Conduct and discipline
- Pensions arrangements
- Injury Benefits
- Recruiting to inward secondments
- Pre-appointment checks for inward secondments

This guidance reflects the Management Code position but the source information can be found here.

Cabinet Office Recruitment Freeze Guidelines This applies to those taken on inward secondment, even if the individual stays on their home organisation's payroll or there is a zero cost agreement.

Civil Service Commission's Recruitment Principles The Civil Service Management Code states that inward secondments must not conflict with rules governing appointment on merit through fair and open competition. The rules allow secondments to be an exception to the Principles but also put a limit of two years on their duration. Secondments recruited via a fair and open competition route will be rare but if this does occur that posting will not be treated as an exception and can be for a period of longer than two years. The link can be found here.

Pre-appointment checks guidance All those moving into the Civil Service on secondment need to have undergone pre-appointment checks. Refer to departmental guidance and the:

- **Baseline Personnel Security Standard,** this sets out the standard security checks across Government and the different clearance level required for different roles. **[DN: Department to insert link to departmental guidance]**

- **Civil Service Nationality Rules,** these apply only to inward secondments where the terms of the secondment agreement are such that the individual is considered to be employed by the Civil Service. These can be found ere.

Annex 2 – Business case template

Employees wishing to apply for a secondment opportunity must satisfy the eligibility criteria set out in the secondments policy and complete the business case template. Detailed information should be provided to enable managers to make an informed decision on whether they are able to support and approve the application.

All sections should be completed in full:

Employee name and grade			
Details of the secondment opportunity: employer, type of business/organisation, role type and working hours			
Duration of secondment			
Details of personal development the opportunity would provide			
Details of business benefits to the home department. For example, skills or knowledge that you will return with.			
Details of business benefits to the wider Civil Service.			
Details of business benefits to the host organisation.			
Outcome (please give reasons for accepting or rejecting the request).			
Manager name and grade			
Signature		**Date**	

Annex 3 - Line manager checklist (outward secondments)

The checklist below can be used to record evidence throughout the secondment process. An up to date copy should be retained which can be reviewed as part of the `Keeping in Touch` process. If there is a change of home manager during the secondment this checklist should be handed to the new manager.

Employee details

Name	
Grade	
Contact details	
Host manager details	
Name	
Business/organisation	
Contact details	
Secondment request	

Have the eligibility requirements been met? (see Secondments Policy)	*Confirm checks and insert details of any issues/concerns.*
Does the business case evidence benefit for the department, the employee, and the Civil Service?	*If yes record date business case approved. If not insert reason refused and date employee informed.*
Does the employee understand the return arrangements? Record details of discussions	

Secondment agreement - Does the employee understand the arrangements for:

Terms and conditions?	
Salary and expenses?	
Keeping in Touch?	
Development reviews?	
Absence reporting arrangements?	
Performance reporting?	
Recording the terms of the agreement?	*Ensure the employee and manager have a signed and dated copy of the agreement.*

Prior to the secondment

What arrangements have been made for filling any vacancy left by the secondment?	
Have you taken action on any HR/payroll changes required e.g. has the employee been recorded as going on secondment?	
Have you undertaken relevant performance action?	
Have you considered reasonable adjustments?	

During the secondment

Are you sending the employee regular communications from the home department as required, e.g. job opportunities?	
When will the keep in touch meetings taking place? Record dates if required.	
Has the employee requested an extension to the secondment?	
Has the extension been agreed?	

Planning for the employee's return

Has a discussion taken place with the employee about return?	
Is the employee's original post still available? If not has an alternative post been found?	
Has the employee's return date been agreed by all parties?	
Do any reasonable adjustments need to be made prior to the employee's return?	

Does the employee require an induction?	
Has the host manager sent over the relevant paperwork and performance reports?	
Has an evaluation of the secondment opportunity and development gained taken place? Record any meeting date(s).	

Post return

Has a further evaluation review been conducted six months after the return date?	

Appendices – Template Secondment Agreements

Appendix 1 – Outward secondment agreement

AGREEMENT FOR SECONDMENT OF CIVIL SERVICE EMPLOYEE TO NON-CIVIL SERVICE ORGANISATION

Warning: this is only a template and must be adapted to suit individual circumstances. Legal advice should be taken where appropriate.

This Agreement is made between:

I. **[Insert name of non-Civil Service (external) organisation]** of [**insert address]** ("the Host")

II. the Department of [**insert Civil Service Department name]** ("the Department")

III. **[insert name of Civil Service employee]** ("the Secondee").

1. Secondment and duration

1.1 The Secondee will be seconded by the Department to work for the Host in the post of **[insert post title**] from **[insert start date]** to **[insert end date].** The Secondees line manager during the secondment will be **[insert name or job title of line manager]**; if a change of line manager is necessary the details will be given to the Secondee and the Department.

2. Status of Secondee; return to Department

2.1 The Secondee will remain the employee of the Department for the duration of the secondment and will not become, or be regarded as, the employee of the Host. If the Secondee ceases to be employed by the Department for any reason during the secondment period then the secondment will terminate immediately.

2.2 At the end of the secondment the employee will return to the home department. The home department will do its best to place the employee in either the same post or another post at the same grade and location as s/he was in before the secondment started, but it cannot guarantee that any post will be available. **[Home departments may wish to make reference to their deployment policies here.]**

2.3 On returning to the Department any terms of the Secondee's contract which were varied because of the secondment will revert back to their original state. Any higher remuneration which applied because of the secondment will cease with the secondment.

2.4 Any temporary promotion linked to the secondment will cease when the secondment ends and the Secondee will return to the Department at their original grade.

3. Location and hours of work

3.1 During the secondment the Secondee's place of work will be **[insert place of work]**.

3.2 The Secondee's hours of work during the secondment will be **[insert working hours]**.

4. Remuneration

4.1 During the secondment the Department will continue to pay the Secondee his/her normal remuneration (including pay for sickness absence, annual leave and pension contributions) **[DN less any department/role specific allowances].** This includes any Departmental pay award which has been made but has not yet come into effect.

OR (if the rate of pay is higher during the secondment)

During the secondment the Department will pay the Secondee at the rate of £ [insert special pay rate if applicable] per annum and will also provide the same benefits as applied before the secondment [or insert here a list of which Departmental benefits will be provided and whether any additional Host benefits will apply. This can be done in an Annex if necessary]. Any departmental pay award which was made before the secondment starts but is not yet effective will not apply.

4.2 The Department will also be responsible for paying PAYE tax and national insurance contributions and any other applicable deductions in respect of the Secondee's remuneration.

4.3 **Pay Awards:** Any pay awards that are implemented within the Department during the secondment should be applied to the Secondees salary as and when they occur.

OR (if the rate of pay is higher during the secondment)

Any pay increases during the secondment will be determined by the Host with the Department's consent. **[DN: a requirement for consent is included so that the Department can prevent any inappropriate increases being granted.]** Any such pay increase will only apply during the period of the secondment. Departmental pay awards will not apply.

On the Secondee's return to the Department his/her salary will be set as follows: **[insert details of how the salary on return will be calculated. E.g. it could be the pre-secondment salary adjusted in line with pay changes which have taken place in the department during the secondment, and based on the box markings (or host equivalents) in appraisals which were done during the secondment. Departmental pay policies may set out what happens about pay on return from a secondment, in which case this clause can refer to the relevant policy.]**

5. Reimbursement

5.1 The Host will reimburse the Department for the full cost of the Secondee's remuneration during the secondment, including any performance-related pay, all benefits, employer's National Insurance contributions and pension contributions. The Host will also pay VAT where applicable on the invoiced amount.

OR (if less than full reimbursement is to be made)

The Host will reimburse the Department for the cost of the Secondee's salary [and …..**[Insert any extras**]. The host will also pay the VAT where applicable on the invoiced amount.

5.2 Reimbursement will be made within **[insert suitable period, e.g. 30 days]** of the Department providing the Host with an invoice giving details of the cost and showing any applicable VAT. Invoices will be presented monthly/quarterly **[delete as appropriate]** in advance/arrears/on the following dates **[delete as appropriate, insert relevant dates].**

[DN: if the pay or reimbursement arrangements are complex it may be appropriate to deal with them in an Annex to the agreement.]

6. Performance Management; performance related pay

6.1 During the secondment the Department will continue to conduct performance reviews of the Secondee and will make decisions about any performance-related pay in accordance with its procedures. If the Host is liable to reimburse the Department for any performance-related pay, the Department must consult the Host before making a decision about such pay.

6.2 The Host will provide the Department with appropriate input for these purposes, to agreed timescales.

OR (delete as appropriate)

Performance reviews during the secondment period will be conducted by the Host under its procedures, with appropriate input from the Department. Decisions about any performance-related pay will be made by the Host under its policies, but will require the consent of the Department. **[DN: this is included so that the department will be able to prevent any inappropriate bonuses being paid.]**

The Secondee will not be entitled to any performance-related pay awarded by the Department.

The Host will assist the Department as appropriate with any post-secondment appraisal which includes work done during the secondment.

[DN: it is important to make sure that the chosen options for whose appraisal and performance systems are used will mesh together properly. In general the party which makes decisions about performance pay should also make decisions about appraisals.]

7. Pension and Injury Benefit Schemes

7.1 The home department that is responsible for automatically enrolling the worker under legislation.

7.2 This secondment will not affect the Secondee's occupational pension arrangements with the Department.

OR

7.3 The pension arrangements during the secondment will be as follows**: [Insert details of changes. The Management Code requires that the Secondee be given a written statement of the effect of the secondment on pension.]**

7.4 This secondment will not affect the Secondee's eligibility for the Civil Service Injury Benefit Scheme. **[If alternative arrangements are being made, this clause will require amendment. The Management Code requires that the Secondee be given a written statement setting out who is providing the benefit and what it comprises.]**

8. Expenses and training

8.1 Any travel, subsistence or other expenses incurred by the Secondee in the course of the secondment will be reimbursed [by the Department in accordance with the rules applicable in that department] or **[delete as appropriate]** [by the Host in accordance with the rules of the Host].

8.2 **[Insert any applicable provisions about who provides and pays for training and development during the secondment.]**

9. Health and safety

9.1 During the secondment the Host will be responsible for the Secondee's health & safety, and will ensure that the Secondee is only required to work for such periods and at such times as are permitted by the Working Time Regulations 1998.

10. Leave and associated pay

10.1 During the secondment the Secondee will continue to be entitled to holiday, sickness absence and other leave (and any associated pay) as provided for in his/her terms and conditions of employment with the Department. At the beginning and end of the secondment any accrued annual leave will be transferred with the Secondee.

OR (delete as appropriate)

During the secondment the Secondee will be entitled to holiday, sickness absence and other leave (and any associated pay) as provided for in the Host's terms and conditions. At the beginning and end of the secondment any accrued annual leave will be transferred with the secondee.

10.2 The Secondee must book leave and report any sickness or other absence to **[insert details]. In some cases it may be appropriate for the Secondee to report to his Departmental line manager <u>and</u> to the permanent Employer]**.

10.3 In **the event the Secondee takes maternity/paternity [DN: delete as appropriate] or adoption leave and:**

The original secondment has not ended prior to return, the Host consents to continue with the secondment and the Secondee has the opportunity to return to the Host organisation to complete the remainder of the secondment period.

The original secondment ends during the period of leave, the Host consents to the Secondee continuing on the agreed secondment terms (if any additional terms were granted) until the secondment period would have finished, had the Secondee not taken **[DN insert type]** leave. At that point, even if the period of leave has not expired they will return to the Home department and move back onto the terms in place prior to the secondment.

11. Standards, including confidentiality and conflicts of interest

11.1 During the secondment the Secondee will observe all the Host's rules, policies and procedures relating to conduct and standards, including confidentiality, unless the Department's rules, policies or procedures require a higher standard, in which case the Secondee will observe that higher standard. This will also apply after the secondment has ended, in relation to any continuing obligations. **[DN: this will cover things like confidentiality, non-dealing or conflicts of interest rules which go further than the home department's policies and which the Secondee must stick to even after the secondment ends.]**

11.2 In the event of any breach of this clause ("Standards, including confidentiality") the Host will inform the Department, and may terminate the secondment early as set out in the termination clause in this agreement.

11.3 The Secondee's attention is particularly drawn to the following Host policies which are attached to this agreement: **[insert details of policies which are specific to the Host in respect of standards and conduct].**

11.4 The Secondee will continue to be bound by the Civil Service Code at all times during the secondment. The same applies to the Business Appointment Rules; these place restrictions on the work which civil servants are able to carry out after leaving the Civil Service and can be found in the Department's staff handbook and in the Civil Service Management Code. The Secondee will also continue to be bound by the Official Secrets Act.

11.5 The Department will not require the Secondee to disclose or use any information which is confidential to the Host, and will keep confidential any confidential information it acquires as a result of the secondment.

11.6 The Host will not require the Secondee to disclose or use any information which is confidential to the Department, and will keep confidential any confidential information it acquires as a result of the secondment.

11.7 If an actual or potential conflict of interests arises during the secondment, any party which becomes aware of the conflict will notify the other parties in writing as soon as possible, and all the parties will attempt to manage the conflict appropriately. If this is not possible the secondment must be terminated in accordance with the termination clause in this agreement.

12. Discipline and grievances

12.1 The Secondee will continue to be subject to the disciplinary and grievance procedures of the Department in respect of matters occurring during the secondment. The Host

will co-operate with the Department in such matters, including by providing any necessary information.

13. Policies and procedures

13.1 Except as otherwise provided in this agreement, the Secondee will continue to be subject to the Department's policies and procedures during the secondment.

OR (if it is more appropriate for the Host's policies to apply)

Except as otherwise provided in this agreement, the Secondee will be subject to the Host's policies and procedures**. [DN consider whether to draw the Secondee's attention here to any major differences between the policies/procedures, or attach the relevant policies. Also consider whether any particular policies of the Host organisation will not be appropriate, such that the Department's policies should apply instead.]**

14. Duty of care

14.1 The Department retains responsibility for the duty of care.

Or [Delete as appropriate]

The Host [insert name] has the duty of care during the secondment.

[DN: The responsibility for duty of care must be mutually agreed]

15. Data protection

By signing this agreement the Secondee agrees to appropriate information about him/her being passed between the Host and the Department and processed by them for employment, managerial, administrative and similar purposes and to comply with legal requirements. Such information will be held securely. Further information about data protection can be found in the Host's staff handbook. **[DN: departments should note that the processing of sensitive data may require more specific consent from the employee.]**

[DN: the Host may wish to review and add further information here.]

16. Early termination

Either the Host or the Department may terminate the secondment for any reason by giving **[e.g. one month]** notice in writing to the other two parties.

16.1 The Host may also terminate the secondment on grounds of serious misconduct by the Secondee, by written notice to the other two parties with immediate effect.

16.2 Either the Host or the Department may terminate the secondment if a conflict of interests arises which cannot be appropriately managed, by written notice to the other two parties with immediate effect.

17. Information and monitoring of leave

17.1 The Host/Department **[delete as appropriate]** will monitor annual leave, sickness absence and other leave. The Host and Department will each provide the other with any information the other needs in order to manage the Secondee, both during the secondment and when it ends. **[It may be appropriate to make provision here for the party that does the monitoring to provide regular reports to the other party about leave and other management matters.]**

17.2 The Secondee must notify both the Host and the Department if his/her home address changes during the secondment.

18. Ethical considerations

18.1 This clause will apply during the secondment and for **[insert suitable period e.g. six months, on which legal advice should be taken]** months after its termination.

18.2 The Host will not induce (or attempt to induce) the Secondee to leave the Department or take up employment with the Host.

18.3 Neither the Department nor the Secondee will induce (or attempt to induce) any of the Host's staff with whom the Secondee has worked to leave the Host or take up employment with the Department.

18.4 This clause will not prevent either the Department or the Host from running general recruitment campaigns or from offering employment to an individual who responds to such a campaign.

19. Liability and indemnities

19.1 The Secondee will work under the supervision of the Host. The Department will not have any liability to the Host for the acts or omissions of the Secondee in the course of the secondment. **[DN: this is to guard against claims being made by the Host if the Secondee does poor work.]**

19.2 The Host will indemnify the Department fully and keep it indemnified fully at all times against any loss, injury, damage or costs arising out of any act or omission of the Secondee in the course of the secondment. **[DN: this is to ensure that the Host and not the Department pays if a third party (including the Host's own staff) makes a claim based on the actions of the Secondee – e.g. if a host employee claims that the Secondee bullied him. The department will remain vicariously liable for the Secondee's actions during the secondment and that is why it could be sued by third parties.]**

19.3 The Host will indemnify the Department fully and keep it indemnified fully at all times against any loss, injury, damage or costs arising out of any act or omission of the Host or its employees, officers or agents relating to the secondment. **[DN: this ensures that the Host should pay if it treats the Secondee badly (e.g. discrimination) or negligently causes him to suffer injury, and the Department has to make a pay-out to the employee or incur other costs as a result.]**

20. Intellectual property

20.1 Any intellectual property which arises in the course of the Secondee's work for the Host shall belong to the Host.

20.2 [DN: If the Department may wish to use any of the intellectual property produced by the Secondee, wording should be added here so that the Host grants the Department a suitable licence to use this and any confidentiality restrictions elsewhere in this agreement are lifted.]

21. Assignment

21.1 This agreement may not be assigned by any party to the agreement without the agreement of the other two parties.

22. Governing law and jurisdiction

22.1 This agreement is governed by and will be construed in accordance with the law of England.

22.2 The parties irrevocably agree that the Courts of England and Wales will have exclusive jurisdiction in relation to any dispute or difference arising out of or in connection with this agreement or its subject-matter or formation (including non-contractual disputes or claims).

23. Variation

23.1 The terms of this agreement may only be varied by agreement in writing between the Host and the Department.

[DN: you may also wish to consider with your legal advisers whether to include additional clauses dealing with service of notices, third party rights and non-waiver of remedies, an "entire agreement" clause and an interpretation clause. Although rarely used you may wish to consider these in relation to your particular business need.]

Signed by:	**On behalf of:**	**Date:**
[insert name of signatory]	**[insert department name]**	
[insert name of signatory]	**[insert host organisation name]**	
[insert name of signatory]	**Employee**	

Appendix 2 – Inward secondment agreement

AGREEMENT FOR SECONDMENT OF INDIVIDUAL FROM NON-CIVIL SERVICE ORGANISATION INTO CIVIL SERVICE DEPARTMENT

Warning: this is only a template and must be adapted to suit individual circumstances. Legal advice should be taken where appropriate.

This Agreement is made between:

I. **[Insert name of seconding non-Civil Service organisation]** of [**insert address]** ("the Employer")

II. the host Department of **[insert Civil Service Department name]** ("the Department")

III. **[Insert name of individual secondee]** ("the Secondee") of **[insert address]**.

1. Secondment and duration

1.1. Appointment to a post in the Home Civil Service ("the Civil Service") is governed by the Constitutional Reform and Governance Act 2010 and the Civil Service Commission's Recruitment Principles issued by the Civil Service Commissioners. The Principles except secondments of up to two years to the Civil Service from the requirement that selection for appointment should be made on the basis of fair and open competition.

1.2. The Secondee will be seconded by the Employer to work for the Department in the post of [**insert post title] [for the purposes of – insert detail here on relevant project or general indication of purpose].** The secondment shall be from **[insert start date]** to **[insert end date]** unless terminated earlier in accordance with this Agreement. The parties may agree to extend the secondment provided that the secondment does not in any event exceed two years in duration.

1.3. The Secondee's reporting manager during the secondment will be **[insert name or job title of line manager]**; if a change of reporting manager is necessary the details will be given to the Secondee and the Employer.

1.4. During the secondment the Secondee will work under the supervision of the Department and carry out all reasonable instructions from the Department. The Secondee will carry out their duties during the secondment in a professional manner and to a professional standard, exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person of their level.

1.5. The Employer will take out and maintain in full force with a reputable insurance company a reasonable level of insurance cover for loss, injury or damage caused to or by the Secondee in connection with the secondment.

1.6. The Secondee will not, without the prior written approval of the Department, do any act, enter into any contract, make any representation, give any warranty, incur any liability or assume any obligation, whether expressly or by implication, on behalf of

the Department, or bind or hold himself/herself out as capable of binding the Department in any way.

1.7. The Secondee will not carry out any work for the Employer during the secondment, except **[DN: insert any exceptions, e.g. attending Employer training or updates or doing small amounts of handover work near the start of the secondment. Be aware of possible conflicts of interest.]**

1.8. The Secondee will remain the employee of the Employer for the duration of the secondment and will not become, or be regarded as, the employee of the Department. If the Secondee ceases to be employed by the Employer for any reason during the secondment period then the secondment will terminate immediately.

1.9. If the Secondee is held to be employed by the Department at any time during the secondment then the Department may dismiss the Secondee and the Employer shall offer the Secondee employment on the terms that applied immediately before that dismissal.

2. Location and hours of work

2.1. During the secondment the Secondee's place of work will be **[insert place of work]**. The Department may require the Secondee to work from other locations as necessary. The Secondee will be informed in advance of any change to the place of work [as long as it remains within reasonable travelling distance].

2.2. The Secondee may be required to travel on the Department's business to such locations and by such means and on such occasions as the Department may from time to time require.

2.3. The Secondee's hours of work during the secondment will be **[insert Departmental working hours]** plus any additional time as may be reasonably required by the Department from time to time.

3. Remuneration

3.1. During the secondment the Employer will continue to pay the Secondee his/her normal remuneration (including pay for sickness absence and annual leave, any variable pay, all benefits, and pension contributions).

3.2. The Employer will continue to be responsible for paying PAYE tax and national insurance contributions and any other applicable deductions in respect of the Secondee's remuneration.

3.3. Any pay rises during the secondment will be determined by the Employer in the normal way**.**

4. Pensions - automatic enrolment

4.1. The Home employer remains responsible for automatically enrolling the employee under legislation.

5. Reimbursement

5.1. The Department will pay the monthly/quarterly **[delete as appropriate]** sum of **[insert monthly or quarterly payment amount]** which represents the Secondee's basic salary and pension contributions as a contribution towards the cost of employing the Secondee, plus VAT if applicable. The Department will not be liable to pay any additional sums (other than the Secondee's expenses, as set out below).

5.2. Payment/reimbursement will be made within **[insert suitable period, e.g. 30 days]** of the Employer providing the Department with an invoice giving details of the payments due and showing any applicable VAT. Invoices will be presented monthly/quarterly **[delete as appropriate]** in advance/arrears/on the following dates **[delete as appropriate/add dates]. [DN consider adding other details such as the address to which invoices should be sent, any reference/purchase order number which must be quoted, etc.]**

5.3. The Employer must ensure that the final invoice covers all outstanding expenditure for which reimbursement may be claimed. The Department will not be liable to pay any items not included in the final invoice.

5.4. [If the Secondee is away from work for any reason for more than **[insert period of time, e.g. six weeks**], the Department's obligation to make payments under clause 5.1 will not apply during that absence.][If this occurs the Department and the Employer will review the secondment, and possible options will include continuing the secondment, ending it on notice or extending it by agreement.] **[DN: both parts of this clause are optional. Note that if a secondment is reviewed, care should be taken not to act in a way which constitutes unjustifiable discrimination, e.g. it may be discriminatory to end a secondment because the secondee is on maternity leave.]**

6. Performance Management; performance-related pay

6.1. During the secondment the Employer will continue to conduct performance reviews of the Secondee in accordance with its procedures. **[If the Department is liable to reimburse the Employer for any performance-related pay, consider including a mechanism for keeping this under control – see note to alternative clause 5.1 above.]**

6.2. The Department will provide the Employer with appropriate input for these purposes as required.

6.3. The Department will assist the Employer as appropriate with any post-secondment performance review which includes work done during the secondment.

6.4. During the secondment the Employer will continue to make decisions about any performance-related pay in accordance with its procedures.

6.5. For the avoidance of doubt, the Secondee will not be paid any performance-related pay awarded by the Department to its own employees.

7. Expenses and training

7.1. Any travel, subsistence or other expenses wholly, exclusively and necessarily incurred by the Secondee in the course of the secondment and in connection with the secondment will be reimbursed by the Department in accordance with its rules and policies provided such expenses are evidenced in such manner as the Department may specify from time to time.

7.2. The Department will allow, in consultation with the Employer, reasonable absence from the Secondee to attend such training courses and other meetings at the Employer's offices as are normally appropriate for a staff member of their level and experience provided that reasonable notice of such training courses and/or meetings is given to the Department. Any such training courses and any related travel expenses will be paid for by the Employer and are not recoverable from the Department.

7.3. Where the Department requires the Secondee to attend training, the Department will meet the costs of such training including the course fees and reasonable travel and subsistence expenses in accordance with its policies.

8. Health and safety

8.1. During the secondment the Department will be responsible for the Secondees health & safety insofar as this is within the Department's control. The Department will ensure that the Secondee is only required to work for it for such periods and at such times as are permitted by the Working Time Regulations 1998.

9. Leave and associated pay

9.1. During the secondment the Secondee will continue to be entitled to holiday, sickness absence and other leave (and any associated pay) as provided for in his/her terms and conditions of employment with the Employer. At the beginning and end of the secondment any accrued annual leave will be transferred with the secondee.

9.2. The Secondee must book leave with and report any sickness or other absence to **[insert details. In some cases it may be appropriate for the Secondee to report to his Departmental reporting manager and to his Employer]**.

9.3. In the event the secondee takes maternity/paternity [DN: delete as appropriate] or adoption leave and:

Secondment has not ended prior to return, the Department will consent to continue with the secondment and the individual has the opportunity to return to the department to complete the remainder of the secondment period.

Secondment ends during the period of leave, the Department consents to the individual continuing on the agreed secondment terms (if any additional terms were granted) until the secondment period would have finished, had the employee not taken leave. At that point, even if the period of leave has not expired they will return to the employer and move back onto the terms in place prior to the secondment.

[DN: The department and the employer are not obligated to extend the secondment but if all parties agree to this due to strong business justification for doing so then this approach may be taken, however it is important to note that secondments which are recruited to as an exception to the commissioners principles are limited to two years.]

10. Standards

10.1. During the secondment the Secondee will observe the provisions of the Civil Service Code (attached), the Official Secrets Acts, and all the Department's rules, policies and procedures relating to conduct and standards, including confidentiality and security, unless the Employer's rules, policies or procedures require a higher standard, in which case the Secondee will observe that higher standard in addition. This will also apply after the secondment has ended, in relation to any continuing obligations (including confidentiality and the Business Appointment Rules).

10.2. In the event of any breach of this clause the Department will inform the Employer, and may terminate the secondment early as set out in the termination clause in this agreement.

10.3. The Secondees attention is particularly drawn to the following Departmental policies which are attached to this agreement:

10.3.1. [Insert list, including e.g. confidentiality, Official Secrets, non-dealing rules, security, the Business Appointment Rules, political activities, conflicts of interest, declaration of interests, hospitality, etc.]

10.4. The Secondee should note that the Business Appointment Rules (which form part of the Civil Service Management Code) may place restrictions on the work which he/she is able to carry out after the secondment comes to an end.

10.5. The Department will not require the Secondee to disclose or use any information which is confidential to the Employer. Any information the department does acquire as a result of the secondment will be kept confidential.

10.6. The Employer will not at any time require the Secondee to disclose or use any information which is confidential to the Department, and will at all times keep confidential any confidential information it acquires as a result of the secondment.

10.7. If an actual or potential conflict of interests arises during the secondment, any party which becomes aware of the conflict will notify the other parties in writing as soon as possible, and all the parties will attempt to manage the conflict appropriately. If this is not possible the secondment must be terminated in accordance with the termination clause in this agreement.

11. Discipline and grievances

11.1. The Secondee will continue to be subject to the disciplinary and grievance procedures of the Employer during the secondment. The Department will co-operate with the Employer in such matters, including by providing any necessary information as required.

11.2. The Department and the Employer will notify each other promptly if they become aware of any disciplinary issue or grievance.

12. Policies and procedures

12.1. Except as otherwise provided in this agreement, the Secondee will continue to be subject to the Employer's policies and procedures during the secondment.

13. Duty of care

13.1. The Employer retains responsibility for the duty of care during the secondment.

Or [Delete as appropriate]

The Department has the duty of care during the secondment.

[DN: The responsibility for duty of care must be mutually agreed]

14. Data protection

"Data Protection Legislation" means "(i) the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679), (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy, and (iii) all applicable law about processing of personal data and privacy, as amended from time to time."

14.1. By signing this agreement the Secondee agrees to appropriate information and personal data (as defined in the Data Protection Legislation as amended from time to time) about him/her being passed between the Employer and the Department and the Department holding, processing and accessing such information and personal data both manually and by electronic means for legal, personnel, employment, managerial, administrative and similar purposes and to comply with legal requirements and central guidance.

14.2. For the purposes of this clause references to "personal data" include "sensitive personal data" as defined by the Data Protection Legislation (as amended from time to time). Sensitive personal data that may be held by the Employer and may be transferred to the Department where necessary will include information about: the Secondee's physical or mental condition, the commission or alleged commission of any offence; any proceedings for an offence committed or alleged to have been committed by the Secondee, including the outcome or sentence in such proceedings; and racial or ethnic origin or religious or similar beliefs (for the purposes of equal opportunities monitoring).

14.3. Such information will be held securely. Further details about data protection can be found in the Department's Staff Handbook. **[DN: check and if necessary amend this clause to ensure that it matches the Department's data protection policy. Departments should also note that processing of sensitive personal data may require more specific consent from the employee.]**

14.4. In the interests of open government and public access to information, the Department may need to disclose details of officials who are on secondment to it

from non-Civil Service organisations, including the Secondee's name, the name and address of the Employer, the nature of the work done and the sums paid to the Employer by the Department. This could be made necessary or desirable by legislation, Parliamentary questions, and requests for information under the Freedom of Information Act, or by central guidance or departmental policy on disclosure. The Employer and the Secondee consent to such disclosure. In deciding what disclosure should be made, the Department will take account of its obligations under the Data Protection Legislation.

15. Early termination

15.1. Either the Employer or the Department may terminate the secondment for any reason by giving [insert a suitable period, e.g. one month] notice in writing to the other two parties.

15.2. The Department may terminate the secondment with immediate effect without notice (or payment in lieu of notice):

15.2.1. On termination of the Secondee's employment with the Employer;

15.2.2. If the Employer is guilty is of any serious or repeated breach of the terms of this agreement; or

15.2.3. If the Employer becomes bankrupt or makes any arrangement or composition with or for the benefit of its creditors.

15.3. The Department may also terminate the secondment on grounds of:

15.3.1. serious misconduct by the Secondee or any other conduct which affects or is likely to affect or prejudice the interests of the Department or is otherwise unsuitable for the work of the Department;

15.3.2. Where the Secondee is unable to properly perform his/her duties by reason of ill health, accident or otherwise for a period or periods aggregating at least [x] working days,

by written notice to the Employer with immediate effect.

15.4. Either the Employer or the Department may terminate the secondment if a conflict of interests arises which cannot be appropriately managed, by written notice to the other with immediate effect.

15.5. [If there is a review of the secondment under sub-clause **[insert number of sub-clause above dealing with long-term absence]** and the Department considers it reasonable to end the secondment early, the Department may terminate the secondment by written notice to the Employer with immediate effect.]

16. Information and monitoring of leave

16.1. The Employer/Department **[delete as appropriate]** will monitor annual leave, sick absence and other leave. The Employer and the Department will each provide the other with any information the other needs in order to manage the Secondee, both during the secondment and after it ends. **[DN: It may be appropriate to make**

provision here for the party that does the monitoring to provide regular reports to the other party about leave and other management matters.]

16.2. The Secondee must notify the Department if his/her home address changes during the secondment.

17. Ethical considerations

17.1. This clause will apply during the secondment and **for [insert suitable period, on which legal advice should be taken]** months after its termination.

17.2. The Department will not induce (or attempt to induce) the Secondee to leave the Employer or take up employment with the Department.

17.3. Neither the Employer nor the Secondee will induce (or attempt to induce) any of the Department's staff with whom the Secondee has worked to leave the Department or take up employment with the Employer.

17.4. This clause will not prevent either the Department or the Employer from running general recruitment campaigns or from offering employment to an individual who responds to such a campaign.

18. Return of property

18.1. At the end of the secondment or at any time on request, the Secondee and the Employer will return all property supplied by the Department and all documents (including copies) which the Secondee has produced, received or obtained in connection with the secondment, and will irretrievably delete any electronic copies thereof. The Employer and Secondee will confirm in writing and produce such evidence as is reasonable to prove compliance with these obligations.

19. Intellectual property

19.1. All Intellectual Property Rights in the output from the Contract shall vest in the Individual who shall grant to the Host department a non-exclusive, unlimited, irrevocable licence to use and exploit the same.

19.2. Subject to this Clause and save as expressly granted elsewhere under the Contract, the Host department shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Individual or its licensors and the Individual shall not acquire any right, title or interest in or to the Intellectual Property Rights of the Host department or its licensors.

19.3. The Individual shall on demand fully indemnify and keep fully indemnified and hold the Host department and the Crown harmless from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Host department and or the Crown may suffer or incur as a result of any claim that the performance by the Individual of the Contract infringes or allegedly infringes a third party's Intellectual Property Rights (any such claim being a "Claim").

19.4. If a Claim arises, the Host department shall notify the Individual in writing of the Claim and the Host department shall not make any admissions which may be

prejudicial to the defence or settlement of the Claim. The Individual shall at its own expense conduct all negotiations and any litigation arising in connection with the Claim provided always that the Individual:

19.4.1. shall consult the Host department on all substantive issues which arise during the conduct of such litigation and negotiations;

19.4.2. shall take due and proper account of the interests of the Host department;

19.4.3. shall consider and defend the Claim diligently using competent counsel and in such a way as not to bring the reputation of the Host department into disrepute; and

19.4.4. shall not settle or compromise the Claim without the prior written approval of the Host department (not to be unreasonably withheld or delayed).

19.5. The Individual shall have no rights to use any of the Host department's names, logos or trademarks without the prior written approval of the Host department.

[DN: if the Secondee is likely to produce any valuable/significant IP, departmental legal advice should be sought on whether this clause should be expanded].

20. Assignment

20.1. This agreement may not be assigned by any party to the agreement without the agreement of the other two parties.

21. Governing law and jurisdiction

21.1. This agreement is governed by and will be construed in accordance with the law of England.

21.2. The parties irrevocably agree that the Courts of England and Wales will have exclusive jurisdiction in relation to any dispute or difference arising out of or in connection with this agreement or its subject-matter or formation (including non-contractual disputes or claims).

22. Variation

22.1. The terms of this agreement may only be varied by agreement in writing between the Employer and the Department.

23. Third Party Rights

23.1. A person who is not a party to this agreement may not enforce any of its terms under the Contract (Rights of Third Parties) Act 1999.

24. Notices

24.1. Any notice given under this agreement shall be in writing and signed by or on behalf of the party giving it and shall be served by delivering it personally, or sending it by pre-paid recorded delivery or registered post to the relevant party at its registered office for the time being [or by sending it by fax to the fax number notified by the relevant party to the other party]. Any such notice shall be deemed to have been received:

24.1.1. if delivered personally, at the time of delivery; [and]

24.1.2. in the case of pre-paid recorded delivery or registered post, [48] hours from the date of posting[; and

24.1.3. in the case of fax, at the time of transmission].

24.2. In proving such service it shall be sufficient to prove that the envelope containing such notice was addressed to the address of the relevant party and delivered either to that address or into the custody of the postal authorities as a pre-paid recorded delivery or registered post [or that the notice was transmitted by fax to the fax number of the relevant party].

25. Indemnity

25.1. The Host shall indemnify the Employer fully and keep the Employer indemnified fully at all times against any loss, injury, damage or costs suffered, sustained or incurred by:

25.1.1. the Secondee in relation to any loss, injury, damage or costs arising out of any act or omission by the Host or its employees or agents [during the Secondment Period]; or

25.1.2. a third party, in relation to any loss, injury, damage or costs arising out of any act or omission of the Secondee [during the Secondment Period OR in the course of carrying out the Services].

25.2. The Employer shall indemnify the Host fully and keep the Host indemnified fully at all times against any claim or demand by the Secondee arising out of their employment by the Employer or its termination during the Secondment Period (except for any claim relating to any act or omission of the host or its employees or agents).]

26. ENTIRE AGREEMENT

26.1. This agreement [together with any documents referred to in it] constitute[s] the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to the Secondment.

26.2. Each party acknowledges that in entering into this agreement it does not rely on, and shall have no remedies in respect of,] any statement, representation,

assurance or warranty (whether made innocently or negligently) that is not set out in this agreement.

26.3. The only remedy available to either party for breach of this agreement shall be for breach of contract under the terms of this agreement.

26.4. Each party agrees that it shall have no claim for innocent or negligent misrepresentation [or negligent misstatement] based on any statement in this agreement.

26.5. Nothing in this agreement shall limit or exclude any liability for fraud.

[DN departments: you may also wish to consider with your legal advisers whether to include additional clauses dealing with service of notices, third party rights and non-waiver of remedies, an "entire agreement" clause and an interpretation clause. Although rarely used you may wish to consider these in relation to your particular business need.]

Signed by:	**On behalf of:**	
Date: [insert name of signatory]	**[insert department name]**	
[insert name of signatory]	**[insert name of employer] [insert name of signatory]**	**Secondee**

This Agreement is made between:

I. **[Insert name of non-Civil Service (external) organisation]** of [**insert address]** ("the Host")

II. the Department of [**insert Civil Service Department name]** ("the Department") III. **[insert name of Civil Service employee]** ("the Secondee").

Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables)

1. Definitions

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

"Buyer Property"	**the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;**
"Buyer Software"	**any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;**
"Buyer System"	**the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;**
"Commercial off the shelf Software" or "COTS Software"	**Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms**
"Defect"	**any of the following:** a) **any error, damage or defect in the manufacturing of a Deliverable; or** b) **any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or**
	c) **any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or**

	d) **any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;**
"Emergency Maintenance"	**ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;**
"ICT Environment"	**the Buyer System and the Supplier System;**
"Licensed Software"	**all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;**
"Maintenance Schedule"	**has the meaning given to it in paragraph 8 of this Schedule;**
"Malicious Software"	**any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;**
"New Release"	**an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;**
"Open Source Software"	**computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;**

"Operating Environment"	**means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:** a) **the Deliverables are (or are to be) provided; or** b) **the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or** c) **where any part of the Supplier System is situated;**
"Permitted Maintenance"	**has the meaning given to it in paragraph 8.2 of this Schedule;**
"Quality Plans"	**has the meaning given to it in paragraph 6.1 of this Schedule;**
"Sites"	**has the meaning given to it in Joint Schedule 1(Definitions), and for the purposes of this Call Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;**
"Software"	**Specially Written Software COTS Software and non-COTS Supplier and third party Software;**
"Software Supporting Materials"	**has the meaning given to it in paragraph 9.1 of this Schedule;**
"Source Code"	**computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;**
"Specially Written Software"	**any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;**
"Supplier System"	**the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and**

	management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions on Intellectual Property Rights for the Digital Deliverables.

3. Buyer due diligence requirements

3.1. The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2. operating processes and procedures and the working methods of the Buyer;

3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2. The Supplier confirms that it has advised the Buyer in writing of:

3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

3.2.2. the actions needed to remedy each such unsuitable aspect; and

3.2.3. a timetable for and the costs of those actions.

3.3 The Supplier undertakes:

3.3.1 and represents to the Buyer that Deliverables will meet the Buyer's acceptance criteria as set out in the Call-Off Contract and, if applicable, each Statement of Work; and

3.3.2 to maintain all interface and interoperability between third party software or services, and Specially Written Software required for the performance or supply of the Deliverables.

4. Licensed software warranty

4.1. The Supplier represents and warrants that:

4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the

Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;

4.1.2. all components of the Specially Written Software shall:

4.1.2.1. be free from material design and programming errors;

4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels and Balanced Scorecard) and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Supplier shall:

5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3. ensure that the Supplier System will be free of all encumbrances;

5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("**Quality Plans**")**.**

6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:

6.4.1. be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

7.1. The Supplier shall allow any auditor access to the Supplier premises to:

7.1.1. inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3. review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.

8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.

8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights

9.1. Assignments granted by the Supplier: Specially Written Software

9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "**Software Supporting Materials**").

9.1.2. The Supplier shall:

9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

a) of its own Existing IPR that is not COTS Software;

b) third party software that is not COTS Software

9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central

Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call-Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2. only use such third party IPR as referred to at Paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5. The Supplier may terminate a licence granted under Paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licensee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) Months:

9.3.4.1. will no longer be maintained or supported by the developer; or

9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 9.2 (to:

9.4.1.1. a Central Government Body; or

9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in Paragraph 9.2.

9.5. Licence granted by the Buyer

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to Paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1. suitable for publication by the Buyer as Open Source; and

9.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3. do not contain any material which would bring the Buyer into disrepute;

9.6.2.4. can be published as Open Source without breaching the rights of any third party;

9.6.2.5. will be supplied in a format suitable for publication as Open Source ("**the Open Source Publication Material**") no later than the date notified by the Buyer to the Supplier; and

9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. Malicious Software

9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. IPR asset management

10.1 The Parties shall work together to ensure that there is appropriate IPR asset management under each Call-Off Contract, and:

10.1.1 where the Supplier is working on the Buyer's System, the Supplier shall comply with the Buyer's IPR asset management approach and procedures.

10.1.2 where the Supplier is working on the Supplier's System, the Buyer will ensure that it maintains its IPR asset management procedures in accordance with Good Industry Practice.

Records and materials associated with IPR asset management shall form part of the Deliverables, including those relating to any Specially Written Software or New IPR.

10.2 The Supplier shall comply with any instructions given by the Buyer as to where it shall store all work in progress Deliverables and finished Deliverables (including all Documentation and Source Code) during the term of the Call-Off Contract and at the stated intervals or frequency specified by the Buyer and upon termination of the Contract or any Statement of Work.

10.3 The Supplier shall ensure that all items it uploads into any repository contain sufficient detail, code annotations and instructions so that a third-party developer (with the relevant technical abilities within the applicable role) would be able to understand how the item was created and how it works together with other items in the repository within a reasonable timeframe.

10.4 The Supplier shall maintain a register of all Open Source Software it has used in the provision of the Deliverables as part of its IPR asset management obligations under this Contract.

Call-Off Schedule 7 (Key Supplier Staff)

1.1 The Order Form lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date and, if applicable, the Statement of Work will list the Key Roles and names of persons who the Supplier shall appoint to fill those Key Roles as of the SOW Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables;

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced;

1.5.6 on written request from the Buyer, provide a copy of the contract of employment or engagement (between the Supplier and Supplier Staff) for every member of the Supplier Staff made available to the Buyer under the Call-Off Contract when providing Deliverables, and under each Statement of Work;

1.5.7 on written request from the Buyer, provide details of start and end dates of engagement of all Key Staff filling Key Roles under the Call-Off Contract and, if applicable, under each Statement of Work[.[; and]

1.5.8 [**Insert** any additional requirements].]

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

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

1. Definitions

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

"BCDR Plan"	1 has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2 has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	3 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"	4 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	5 has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	6 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	7 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	8 has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	9 has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

2.1 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.

2.2 At least ninety (90) Working Days after 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:

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

2.2.2 the recovery of the Deliverables in the event of a Disaster

2.3 The BCDR Plan shall be divided into three sections:

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

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

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

2.4 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 the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

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

3.1.2 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;

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

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

3.1.5 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;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

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

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

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

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 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;

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

3.1.12 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.

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

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

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

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

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

3.3 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.

3.4 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.

4. Business Continuity (Section 2)

4.1 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:

4.1.1 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

4.1.2 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.

4.2 The Business Continuity Plan shall:

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

4.2.2 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;

4.2.3 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

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

5. Disaster Recovery (Section 3)

5.1 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.

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

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

5.2.3 loss of the Supplier's helpdesk or CAFM system;

5.2.4 loss of a Subcontractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

5.2.10 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;

5.2.11 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;

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

5.2.13 testing and management arrangements.

6. Review and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

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

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

6.1.3 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.

6.2 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.

6.3 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.

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

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices 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.

7. Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

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

7.1.2 in the event of any major reconfiguration of the Deliverables

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

7.2 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.

7.3 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.

7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with 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.

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

7.5.1 the outcome of the test;

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

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

7.6 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.

8. Invoking the BCDR Plan

8.1 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.

9. Circumstances beyond your control

9.1 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.

Joint Schedule 3 (Insurance Requirements)

1. The insurance the Supplier needs to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for the Contract Period and for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other

evidence of placing cover representing any of the Insurances to which it is a party.

3. What happens if the Supplier is not insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. Evidence of insurance to be provided

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. Required amount of insurance

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in

dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following insurance cover from the Framework Start Date in accordance with this Schedule:

1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);

1.2 public liability and products insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and

1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2. Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3. Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff to lodge deposits or identify papers with the employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world;

3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world;

3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;

3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. Income Security

4.1 The Supplier shall:

4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;

4.1.3 ensure all workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. Working Hours

5.1 The Supplier shall:

5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

5.1.3 ensure that use of overtime used responsibly, taking into account:

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

1.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

1.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

1.3.1 this is allowed by national law;

1.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

appropriate safeguards are taken to protect the workers' health and safety; and

1.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

1.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

2. Sustainability

2.1 The Supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled, unless the Buyer states to the contrary, to sub-contract its obligations under each Call-Off Contract to the Key Subcontractors set out in the Call-Off Order Form.

1.2 Subject to Paragraph 1.1, the Supplier is entitled to sub-contract some of its obligations under a Call-Off Contract to Key Subcontractors who are specifically nominated in the Order Form.

1.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-Contract or replace a Key Subcontractor, it must obtain the prior written consent of the Buyer and the Supplier shall, at the time of requesting such consent, provide the Buyer with the information detailed in Paragraph 1.4. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. The Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

1.4.2 the name and details of the directors, employees, agents, consultants and contractors of the subcontractor engaged in the performance of the Supplier's obligations under the Contract. Details should include: name; role; email address; address; contract details; Worker Engagement Route – for example, employed by subcontractor; engaged via worker's intermediary e.g. PSC (i.e. a personal service company), engaged as an independent sole trader or employed by another entity in supply chain;

1.4.3 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.4 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's length" terms;

1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and

1.4.6 (where applicable) the Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

1.5 If requested by CCS and/or the Buyer, within 10 Working Days, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

(d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the buyer can end this contract) and 10.5 (When the supplier can end the contract) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to

the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default: Deadline for receiving the	[**Guidance:** Explain the Default, with clear Schedule, Clause and Paragraph references as appropriate] [**add** date (minimum 10 days from request)]		
[Revised] Rectification Plan:			
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default Anticipated impact	[**add** cause] [**add** impact]		
assessment:			
Actual effect of Default: Steps to be taken to	[**add** effect] **Steps**	**Timescale**	
rectification:	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete	[X] Working Days		
rectification of Default			
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review Reasons for rejection (if applicable)	[Plan Accepted] [Plan Rejected] [Revised Plan Requested] [**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 13 (Cyber Essentials Scheme)

1. Definitions

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

"Cyber Essentials Scheme"	the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme can be found at: https://www.cyberessentials.ncsc.gov.uk/
"Cyber Essentials Basic Certificate"	the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
"Cyber Essentials Certificate"	Cyber Essentials Basic Certificate or the Cyber Essentials Plus Certificate to be provided by the Supplier as set out in the Order Form
"Cyber Essential Scheme Data"	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
"Cyber Essentials Plus Certificate"	the certification awarded on the basis of external testing by an independent certification body of the Supplier's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2. What Certification do you need

2.1 Where the Framework Award Form and/or Order Form requires that the Supplier provide a Cyber Essentials Plus Certificate prior to Framework Start Date and/or commencing the provision of Deliverables under the Call-Off Contract including, if applicable, any Statement of Work, the Supplier shall provide a valid Cyber Essentials Plus Certificate to CCS and/or the Buyer. Where the Supplier fails to comply with this Paragraph it shall be prohibited from commencing the provision of Deliverables under the Call-Off Contract until such time as the Supplier has evidenced to CCS and/or the Buyer its compliance with this Paragraph 2.1.

2.2 Where the Supplier continues to process data during the Call-Off Contract Period the Supplier shall deliver to CCS and/or the Buyer evidence of renewal of the Cyber Essentials Plus Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.

2.3 In the event that the Supplier fails to comply with Paragraph 2.1 or 2.2, CCS and/or the Buyer reserves the right to terminate the Call-Off Contract for material Default.

2.4 The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process Cyber Essentials Data contain provisions no less onerous on the Subcontractors

than those imposed on the Supplier under the Call-Off Contract in respect of the Cyber Essentials Plus Scheme under Paragraph 2.1 of this Schedule.

2.5 This Schedule shall survive termination or expiry of this Contract and each and any Call-Off Contract.

Ministry of JUSTICE | HumanResources Directorate

Conduct Policy

August 2012

Ministry of
JUSTICE

Contents

Ministry of
JUSTICE

Introduction

Thispolicygivesallofourpeopleinministryof Justice(MoJ) information onthebehaviourand conductweexpectfromyouwhileworkingforus. It highlights your main responsibilities as an employee and as a civil servant.

Our aimisto make workingfor Ministry of Justice a positive experience by encouraging good behaviourandconduct,andtoclearlyexplainthe consequencesof not meeting the standardswe expect.

Section 01

Ministry of JUSTICE

Section 02

Policy

2.1 Who does it apply to?

This policy applies to all permanent and fixed-term employees in the Ministry of Justice (MoJ)includingmembersoftheSCSinthe NOMS businessgroup(but notthosebelow SCS inthe NOMS business group). It covers all levels of seniority and length of service. It applies to everyone in the same way.

If you workfor us under a contractyou will also be expected to keep to this policy. This includes agencyworkers,consultantsandcontractorsand interimstaff.However,ifyourconductfallsbelow thestandardsweexpect,wewilldealwiththis under theterms of the contract under whichyou provide yourservices.

This policydoes notforma partofyour contract of employment. However,you are bound bythe conditionsofthispolicywhichwemayamend from timeto time.

2.2 Principles

We want to see a positive commitment to high standards of behaviour and conduct from all our employees. This is so we can carry out our business functions successfully.

Our standards (see 2.3 below) are built on what the public expects from those who provide services to them. They take account of:

- the values and standards expected of all civil servants – described in the *Civil Service Code*;
- other rules that affect all civil servants (such as confidentiality and official information, appropriate behaviour and political activities); and
- conduct which meets our organisational values, including not accepting any unfair form of discrimination.

If you fail to meet these standards, it undermines our work and we will deal with it using our disciplinary procedures.

This *conduct policy* does not contain details of all rules and standards that apply to employees. You can find these in other documents such as the *Security handbook*, *IT Usage Guidance*, *Smoke-free policy*, *Drugs and alcohol guidance*, *Whistleblowing guidance*, *Information assurance guidance* and *Health and safety guidance*. All of these reflect mutual trust and respect between us and each employee.

If you are a member of the SCS in the NOMS (HMPS) business group, a number of NOMS (HMPS) policies and processes will also apply to you including PSO 8460 set out on the Conduct and Discipline website:

- PSO 8610 Staff Alcohol Policy
- PSO 8550 Grievance Policy
- PSO 8605 Reporting Wrongdoing
- PSO 8100, PSI 23/2000 and the NOMS (HMPS) Security Vetting website on Racist Group Membership
- PSO 8650 Travel and Subsistence Policy
- PSO 7500 Finance Manual
- PSO 1310 Anti Fraud Strategy
- NOMS health and safety guidance, all of which are available on the HM Prison Service intranet.

Prison Service Orders are at: http://www.hmprisonservice.gov.uk/resourcecentre/psispsos/listpsos/

23 Standards of behaviour

Principle

These are the standards of conduct and behaviour we expect every employee to meet.

If youdo not meet all ofthese standards, your manager may take action under the disciplinary procedure.

You will:

- carry out your duties following the civil service values (honesty, integrity, objectivity and impartiality–for more informationsee www.civilservice.gov.uk);
- take responsibility for your actions;
- treat people decently and with respect;
- takecareofallofficialpropertyforwhichyou are personallyresponsible,andimmediately report toyourmanageranylossordamage;
- bepolite, reasonableandfairinyourdealings withpeoplewhouseourservices(prisoners, court and tribunal users, defendants, witnesses, the publicand soon) and colleagues; and
- keeptopoliciesandprocedureswhichrelate toyourbusiness area, includingpolicieson security,therulesinthispolicyand specific rules such as prison service rules on relationships withprisoners.

You will not:

- discriminateagainstanypersonorgroupfor anyunfairreason(includingtheirrace,ethnic or nationalorigin, sex, sexualidentity,sexual orientation,maritalorcivilpartnershipstatus, age, disability, religion or belief, caring responsibilities, working pattern or trade-union membership); or
- harass, victimise orbullyothersthroughyour actions,languageorbehaviour(whetherdone deliberately ornot).

Zero tolerance

This means we will:

- alwaysinvestigateandtreatallegationsof unacceptablebehaviourseriously;and
- takeactionappropriatetohowseriousthe break of the policy is.

What is unacceptable behaviour?

Harassmentisunwantedbehaviourwhichaffects aperson'sdignity.Itcanrelateto age,sex,race, disability, religion, nationality or any other personalcharacteristicoftheindividualand may becontinuousoraone-offincident.Basically,the actions or comments are seen by the person receivingthemasdemeaningandunacceptable.

Bullyingmayincludeoffensive,intimidating, maliciousor insultingbehaviouror anabuseor misuseofpowerwhichaimstoundermine, humiliate or injure someone.

Bullying or harassment may be by an individual againstanindividualor involvegroupsofpeople.

Victimisationiswhenan individualistreatedin a negativewaybecausetheymakeacomplaint, plan to make a complaint, or have helped someone elseto make a complaint.

Examples of unacceptable behaviour

Unacceptable behaviour may include:

- spreadingmaliciousrumours,orinsulting someone;
- unwantedcontactsuchasverbalabuseor offensive gestures;
- unwanted physical contact (including unnecessarytouching,andphysicalthreatsor assaults);
- misuse of poweror position such as making impossible workdemands or providingtoo muchunnecessarysupervision;
- unfair treatment;
- isolatingsomeone or encouragingthemtodo somethingillegal or unacceptable;

- ridiculing or demeaning someone, teasing them or making them the target of pranks or practical jokes;
- inappropriately commenting on a person's appearance, personal life or lifestyle; or
- displaying literature, pictures, films, videos or CDs or other items that could offend.

This is not a full list. You should remember that unacceptable behaviour related to harassment, bullying and victimisation could take place face-to-face, on the phone, by email or letter.

Please see section 3.3 and *IT Usage Guidance* for more information about your responsibilities when using the internet and emails.

If you are not sure what is acceptable, you should get advice from your line manager or your manager's manager.

2.4 Reporting concerns

We are committed to having an ethical work environment. If you see any conduct which does not meet the standards in this policy, or believe you are being asked to act in a way which goes against the *Civil Service Code*, you should normally report your concerns to your line manager or your manager's manager.

They will decide on the best way to deal with the complaint, which could include mediation or, if this is not possible or has been tried and has failed, using the appropriate disciplinary policy.

- If you are a member of the SCS in the NOMS business group, your managers will follow the policy and processes set out in the NOMS (HMPS) Conduct and Discipline website.
- If you are not a member of the SCS in the NOMS business group, your managers will follow the *Discipline policy*.

If you feel you need to make a complaint, you may do so using the appropriate grievance policy.

- If you are a member of the SCS in the NOMS business group, you should follow the guidance at PSO 8550 Grievance Policy on the HM Prison Service website.
- If you are not a member of the SCS in the NOMS business group, you should follow the *Grievance policy*.

Prison Service Orders are at: http://www.hmprisonservice.gov.uk/resourcecentre/psispsos/listpsos/

In instances where this is not possible or appropriate, you may need to report the matter using the *Whistleblowing guidance*.

2.5 Breaking this code

If your conduct and behaviour does not meet the high standards set out in this policy, your manager will take appropriate action to stop the misconduct continuing and to prevent it from happening in the future. Managers will use the discipline procedure if they feel that it is necessary. If you keep breaking the *conduct policy*, or you break it in a serious way, you may receive a formal warning or be dismissed without notice.

If you are a member of the SCS in the NOMS (HMPS) business group, your managers will follow the policy and processes set out in the NOMS (HMPS) Conduct and Discipline website if they feel disciplinary action is needed.

Prison Service Orders are at: http://www.hmprisonservice.gov.uk/resourcecentre/psispsos/listpsos/

26 Responsibilities

As an employee or a person working for us under a contract (including agency workers, contractors and so on) you will:

- read and understand this policy and keep to its standards and rules;
- follow the organisational values and the principles of the *Civil Service Code* which are in this policy;
- ask your manager to explain any parts of the policy you are not sure about; and
- include and promote equality and diversity in all that you do.

As a manager you will:

- set a positive example for your staff in both your managerial and professional behaviour, which is appropriate to your level of responsibility;
- include and promote equality and diversity in all that you do;
- put the standards of this policy into practice and deal with any problems fairly (you have a responsibility to take appropriate action to make sure that we maintain standards within your immediate work area and outside of MoJ);
- make sure that the members of your team are properly inducted and are aware of and understand their personal responsibilities to meet the standards in this *conduct policy;*
- monitor their behaviour to make sure they keep to the policy and, where necessary, explain to your team all parts of this policy to improve their understanding;
- take complaints seriously and take appropriate action, as soon as possible, to deal with anyone who does not keep to this policy; and
- if appropriate, make sure that members of the SCS in the NOMS business group are aware of the NOMS (HMPS) policies that apply to them.

Human Resources will:

- make sure this *conduct policy* is available to all staff by providing it to all new staff and making sure that it is referred to in induction guidance;
- support managers' and employees' understanding of this policy by providing advice and training; and
- monitor how effective this policy is by:
  - gathering, analysing and, where possible, publishing statistics on warnings and dismissals as a result of people breaking this policy;
  - reviewing relevant responses from the staff opinion survey; and
  - reviewing confidential reporting (whistleblowing) cases.

Ministry of JUSTICE

Section 03

Rules

3.1 Gifts, hospitality and reward

Principle

You will not accept gifts or hospitality, or receive other benefits. In particular you are breaking this policy if you accept any gift or payment for:

- **doing, or not doing, anything in your official capacity; or**
- **showing favour (or the opposite) to any person in your official capacity.**

If you do not keep to the conditions, your manager may take action under the disciplinary procedure.

You are not allowed to accept gifts, hospitality or other benefits. This is because accepting these rewards could affect or influence your judgement, or cause your official role to conflict with your personal interests.

There are exceptions to this rule for gifts which are generally seen as inexpensive and hospitality in the form of refreshments during meetings. You will decide (with your manager where appropriate) whether accepting gifts and hospitality is acceptable.

You will report all offers of gifts, hospitality and awards to your manager whether or not you accept the offers. You will do so in line with the financial rules for your business group.

If you are a member of the SCS in the NOMS business group, use the guidance in:

- the SCS Staff Handbook PSO 7500; and
- Finance Manual and PSO 1310 – Anti Fraud Strategy.

Prison Service Orders are at: http://www.hmprisonservice.gov.uk/resourcecentre/psispsos/listpsos/

If you are not a member of the SCS in the NOMS business group, use the *Gifts and hospitality policy and procedures* on the intranet at: http://intranet/justice/corporate-news/office-notices/files/2008/2008-06-30.htm.

Special considerations apply to gifts and hospitality from overseas governments or organisations. Although the principles set out above generally apply, there may be times when refusal could appear impolite, or you should offer a gift in return. You should discuss these offers with your manager if you are not sure whether or not to accept the gifts or hospitality.

32 Drugs and alcohol

Principle

We will, where appropriate, be supportive when dealing with you if you are dependent on, or addicted to, drugs or alcohol.

This means that if you need help for a substance-misuse problem, we will not end your employment simply because of your addiction.

However, if your performance, attendance or behaviour is unacceptable, despite any support and help that we can offer, we may have to dismiss you.

There will be circumstances where we will treat breaking the policy, whether dependency-related or not, as a disciplinary matter and we may dismiss you. Examples include if you:

- deliberately ignore personal safety by drinking alcohol or taking drugs;
- take part in unacceptable behaviour in the workplace associated with drinking alcohol or taking drugs;
- are found incapable of carrying out your normal duties satisfactorily as a result of drinking alcohol or taking drugs;
- drink alcohol or take drugs at work or when on call and likely to be called to work at short notice;
- possess, take, deal, sell or store controlled drugs either on work premises or are involved in these activities outside of work;
- are disqualified from driving as a result of alcohol or drug-related offences (if, under your contract of employment, you have to drive a vehicle); or
- make malicious or untrue allegations that a colleague is drinking alcohol or taking drugs.

This is not a full list. We will take disciplinary action, in all cases, which is appropriate to the circumstances.

If we have enough evidence, we will tell the police about illegal drug use or of any illegal activity or behaviour. For example, we would need to report criminal behaviour associated with alcohol abuse, such as having a drink-driving accident in a work vehicle.

If you are a member of the SCS in the NOMS business group, you are not allowed to drink while at work. Your staff in grades below SCS level must be 'fit for work'. The standard of being 'fit for work' within NOMS (HMPS) below SCS level is defined as being within the drink-driving limit. Your manager could ask you to take a test if they have reason to believe that you are breaking the rules of the policy. You can find further guidance in:

- PSO 8610 Staff Alcohol Policy; and
- PSI 14/2006: Guidance for Managers.

Prison Service Orders are at: http://www.hmprisonservice.gov.uk/resourcecentre/psispsos/listpsos/

If you are not a member of the SCS in the NOMS business group, you can find further guidance in *Drugs and alcohol guidance* or you can contact Workplace Support on 0121 681 3475.

33 Using IT systems, phones, fax and mail

Principle

You will not visit illegal or unacceptable internet sites or play games, and you will not write or send illegal or unacceptable emails or letters.

You will not allow your personal use of IT systems and the phones to affect your work performance or to take priority over your work duties.

If you do not keep to these conditions, your manager may take action under the disciplinary procedure.

IT systems

We provide email, intranet and internet and other IT facilities for business use, to help you to do your job effectively and efficiently. You and your manager are responsible for making sure that you keep to the rules set out by the Operational Security Team or the IT policies that apply to your business group.

You can use the internet for legal purposes as long as:

- you do so during non-work time only, for example during your lunch or a recognised break;
- it does not affect your work performance or take priority over your work duties; and
- you keep to the requirements of the *IT Usage Guidance*.

We do not allow personal use outside of these times unless you have your line manager's permission.

If you break the policy, we can take disciplinary action. For example, if you download, view, display or forward offensive or indecent material, this is gross misconduct and you could be dismissed.

If you receive any of this material, you will immediately report it to IT security in your business group and delete it. If you fail to do so, you will have broken the policy.

If you are not sure what is acceptable and unacceptable use of IT systems, you should get advice from your line manager.

We may review and monitor your use of the IT systems under the Lawful Business Uses Regulation of the *Regulation of Investigatory Powers Act (RIPA) 2000* if we suspect excessive personal, or inappropriate use. In these circumstances, we will normally warn you beforehand.

For more detailed guidance, please see the *IT Usage Guidance*.

Using phones

We provide phone equipment for business use.

You can make short, urgent phone calls that you cannot leave until lunch, recognised breaks, or after work. However, you will keep these to a minimum and they will not interfere with your duties.

We may review and monitor phone calls under the Lawful Business Uses Regulation of the *Regulation of Investigatory Powers Act (RIPA) 2000* if we suspect excessive personal or inappropriate use. In these circumstances, we will normally warn you beforehand.

You will normally switch your mobile phone to silent while you are working to make sure that you do not disturb customers or team members.

Post and faxes

We provide a postal system and fax machines for business use only. You will never put unstamped personal letters through the postal system we pay for or put personal documents through the fax machine.

3.4 Dress

Under the *Civil Service Code* you will :

'alwaysact inawaythatis professional andthatdeservestheconfidenceofall those you deal with'.

In some instancesour customers will expect us to present a smart or professional appearance while at work or on official business. If there is a particular business need, you may needto follow a certain dress code.

In these circumstances, managers should:

- make surewedonotdiscriminatefor any reason;
- considerwhatisappropriatedressto meetthe business need and avoidbeing unnecessarily strict;
- rememberthatifanemployee'sreligionmeans theymustfollowaparticulardresscode,this must berespected;
- makesurethat,ifnecessary,employeeswear identificationbadgesorsecuritypasses;and
- givestaffuniformsifneeded,forexample, gownsfor court ushers.

Youwillnot wearbadgesordisplayslogansor anything which shows you are a member of a particularpoliticalparty.Youmaywearsmall badges showingyour membershipof acivilservice trade union.

Becausewehaveanumber ofbusinessneeds, we donothaveastandarddresscode. Asaresult,this guidanceismeanttoprovideaframeworkonly. Askyour manager whatdresscodeisinplacein your workplace. Your managers will normally discussyourdresscodewithlocaltrade-union representatives.

3.5 Dealingwithofficial information

Principle

Youwillnotreleaseofficialinformationunless you are authorised to do so.

Ifyoureleaseofficialinformationwithout authority, yourmanagermaytakeaction underthedisciplinaryprocedure.

We encourageopenness andfollowthe principle thatweshouldmakeofficialinformationavailable tothepublicunlessitisclearlynotinthepublic interest to do so. However, there are some restrictionsonwhatyoucan release.Youwillnot release, to anyone who is not authorised to receive it, personal sensitive information or informationyou havegainedthroughyourofficial duties.

If you are not sure, ask your manager before releasinganyinformation.Ifyoureceivearequest for information, youcan also contactthe **Access Rights Unit**for more advice. Ifyouwanttorelease information, you should discuss how to do so with thepressofficeormediarelationsbeforehand.

You will:

- takeparticularcarewithinformationwhichhas a securitymarking–formoreinformationon security markings and howthisaffectshowyou handle information, ask your manager or contact securitybranch;
- confirmtheidentityofanyoneaskingfor information(perhapsbycallingthemback) beforedecidingifitshouldbereleased;
- askforpermissionbefore becoming involvedin any activity which might lead to revealing official information or use your official experience(forexample,beforetakingpartin discussionsor seminarsoutsideof MoJ);

- use personal or sensitive information in line with the *Data Protection Act 1998* – for more guidance contact the Access Rights Unit;
- clear, beforehand, text for publication which uses official information or experience; and
- not try to obstruct or hold up policies or decisions by revealing, outside government, any information you have had access to.

These obligations continue after you have left the service. See the section in this policy on *Outside appointments* at 3.15 for more details. See also the section on *Taking part in trade-union activities* at 3.13.

3.6 Press, TV or radio

Principle

You are expected to support our aims and achievements, but must leave dealing with the media to staff in the press office or media relations who have specific responsibility for this.

If you do not do this, your manager may take action under the disciplinary procedure.

If the press and media ask you for information, you should refuse their request and give them the name of the appropriate, authorised person for a response. This would normally be someone from the press office or media relations or a senior manager (area director, regional director, or equivalent). If you are not sure who the appropriate person is, ask your manager. If you are taking part in trade union activities, you must follow the rules in section 3.13.

3.7 Publications

Principle

You will get permission before revealing information you have access to as a result of your job.

If you do not get permission, your manager may take action under the disciplinary procedure.

You need permission before you publish electronically or in hard copy, a book, article, letter, or any other publication including film, video or audio material that relates to our official business or another government department. You should send an outline of the proposed work to the following for their permission.

- If you are a member of the SCS in the NOMS business group, send it to HR Policy and Reward.
- If you are not a member of the SCS in the NOMS business group, send it to your senior manager (area director, regional director or equivalent).

You will then send the finished text for approval before you publish it. If the publication is likely to interest the media or is political, you should also contact the press office or media relations for advice. You cannot receive payment for a publication produced in work time.

Your publication may be covered by Crown Copyright protection. Crown Copyright applies to any work which you have prepared or published in the course of your employment. This means that copyright belongs to the Crown and not you as the author. As a result you will not be entitled to payment or reward if the work is published or marketed. For more information, contact the Office of Public Sector Information (OPSI).

You must not publish or broadcast your personal experiences (memoirs) in government, or enter into commitments to do so, while we employ you. You must ask the permission of the Permanent Secretary and the Head of the Home Civil Service, before entering into a contract to publish these memoirs after leaving the service.

You should send your proposed memoirs in good time before any proposed publication date. In reviewing information, the Permanent Secretary and the Head of the Home Civil Service will take account of whether the information could damage international relations, national security or the confidential relationships between ministers, and between ministers and civil servants.

If you are appointed to a sensitive post, as a condition of taking up the post, we will assume you have transferred to the Crown, copyright in any future work which relates to your employment or which contains or relies on official information which you became aware of as a result of your employment as a civil servant. If the Permanent Secretary or the Head of the Home Civil Service give permission to publish the work, we will transfer copyright in the relevant part of the work.

3.8 Speeches and lectures

Principle

You will get permission before speaking publicly on any subject that relates to your work or official business.

If you do not get permission, your manager may take action under the disciplinary procedure.

You will get permission from a senior manager (head of section, area director, or equivalent) before giving a speech or lecture outside of work that relates to your work or official experience unless you are a member of NOMS (HMPS) Senior Civil Service and have been given authority to accept invitations to give talks and lectures. If the speech or lecture is likely to interest the media, or is political, you should also contact the press office or media relations for advice. If asked to give speeches or lectures at events arranged by political parties, you will keep to the *Political activities* section of this policy (see 3.16).

You cannot be paid for a speech or lecture that relates to your work or official experience. For more guidance, see *Gifts, hospitality and reward* guidance at 3.1. You can claim reasonable travel, food and accommodation costs.

3.9 Takingpartinsurveys

Principle

Youwillgetpermissionbeforetakingpartin surveysonanysubjectthatrelatestoour business.

Ifyoudo not get permission, yourmanager may take action under the disciplinary procedure.

Youcantakepartinanysurveysoutsideofwork that are notconnectedtoofficial matters. If the surveyrelatestoofficialmattersorisaimedat gatheringofficialviews,youwillaskforpermission fromaseniormanager(headofdivision,area director,or equivalent)beforetakingpart.

Youwillnormally be given permission as long as theinformation isfactualandalreadyinpublic circulation.

Inyourofficialcapacity, if you are askedtotake part in surveys which deal with attitudes or opinionsonpoliticalmattersormattersof policy, youwillkeeptotherulesin *Politicalactivities*, section 3.16 of this policy.

3.10 Fraud

Principle

You will act with honesty at all times and protect the public resources you are responsible for.

Ifyoudonot, wemaytakeactionunderour disciplinary or fraud-investigationprocedures.

Fraudisacriminaloffenceunderthe*FraudAct2006*, whichcame intoforceon 15 January 2007.There arethree waysinwhichfraudcan becommitted:

- false representation;
- failuretorevealinformationwhenthereis a legal dutyto do so; and
- abuse of position.

Ineachcaseapersonmustplantomakeagainfor themselvesor another,ortocauselossto another, orexposeanothertoariskofloss.The*FraudAct* appliestooffencescommitted in England, Wales and Northern Ireland, but does not include Scotland.

We will investigate any casewe suspectinvolves fraud or corruption. You are responsible for preventing fraud and will use preventative measurestoreduceandmanagetheriskoffraud.

- If youareamember of the SCS in HMPS in the NOMS business group, see PSO 1310– Anti FraudStrategy.
- IfyouarenotamemberoftheSCSinthe NOMS business group, use the guidance at section 13 of the *FinanceManual*.

Prison Service Orders are at: http://www. hmprisonservice.gov.uk/resourcecentre/psispsos/ listpsos/

3.11 Personal affairs

Principle

You will not put yourself in a position where you have a conflict between your duty and your private interests. If this happens, you will report it to your manager.

You will be sensitive to the public view that these kind of conflicts could prevent you from being impartial when carrying out your duties.

If you do not do so, your manager may take action under the disciplinary procedure.

You need to be, and to be seen to be, independent, honest and fair when carrying out your duties. You also need to be careful in your private life so you do not do anything which might conflict with your duties. This doesn't mean that we do not respect your right to a private life as set out in the *Human Rights Act*. However, you need to let your manager know about anything in your private life (for specific, examples see A to E below) that may affect your official duties.

A – Conflict of interest

If you think there may be a conflict of interest between your official duties and something in your private life, you will report it to your manager. You will be sensitive to the public's view that the conflict could prevent you from carrying out your duties fairly or that you may be suspected of improper behaviour. You will not use your position to favour (or the opposite) someone based on:

- your personal interests, relationships, friendships, associations, membership of societies, clubs and other organisations (such as being a Freemason); or
- the interests of your friends, relatives or anyone you have a close personal relationship with.

B – Contracts

You will not make a bid for a contract we have put to tender either personally or through an organisation in which you have a financial interest unless you have revealed this interest and you have permission. You should ask your manager, your head of division, area director, or equivalent and your HR Case Manager for permission in the first instance.

If, while at work, you come into contact with any matter to do with a business organisation you have an interest in, you should reveal this to your manager, head of division, area director, or equivalent, and HR Case Manager and ask that another member of staff deals with the matter.

C – Personal financial affairs

You may invest in shares and other investments unless it conflicts with the nature of your work. You will not be involved in taking any decisions which could affect the value of your private investments, or the value of those on which you give advice to others. And you will not use information you have gained in the course of your work for your own private financial interests or those of others.

You will report to your manager:

- business interests (including directorships) or shares or other investments you or members of your immediate family hold which you would be able to gain from as a result of your official position; and
- if you are in financial difficulties and legal action (for example, a county court judgment) is taken against you, or you become bankrupt or insolvent.

Yourmanagerormanager'smanagerwillconsider:

- theeffectyouractionsarelikelytohaveonhow effectiveyouareatspecificdutiesortowork for us;
- the risk to public money; and
- whetherwewill beaffectedinanegative way.

Wewilltakedisciplinaryactionagainstyouif:

- youhavedone somethingdeliberately which has affected our reputation;
- you havefailedto tell your manager or HR Case Manager about youractionsor involvement; or
- thereisevidencethatpublicfundsmayhave been involved in an illegal act.

D – Commercially sensitive information

Ifyouhaveaccesstoinformationthatcouldaffect the price of the shares or investments of a particularcompany, it is an offenceto:

- dealinthosesharesorinvestments;
- giveadviceaboutor arrangesuchadeal;or
- passon information to be usedforthe purpose ofdealing, givingadvice aboutorarrangingа deal.

Ifyou are notsureaboutyourposition, askyour manager.

E–Reportingarrestsorcriminalconvictions

Youwillletyourmanagerknowimmediatelyif you are arrested, imprisoned, charged, or convictedofanycriminaloffence,orifyoureceive a policecaution,summonsorreprimand.Your manager willthentellyourheadofdivision, area director,orequivalent, and HRCase Manager. If youdriveaspartofyournormalworkingduties, you will let your manager know immediately about any traffic offences (except parking offences)or disqualificationfromdriving.

Other action taken will depend on:

- the nature of the offence;
- the outcome of court proceedings;
- the effect on our reputation; or
- theeffectonyourabilitytodoyourjob effectively.

3.12 Other employment

Principle

You may take on other work as long as:

youdeclareyourplansbeforestartingthe work;

it doesnot conflictwithyourduties; and

youhavebeengivenpermissionto do so.

If you do not do this, your manager may take actionunderthedisciplinaryprocedure.

You will get written permission from your manager beforetaking upanotherjob,whether paidorunpaid,whileyouareemployedbyus. This isbecauseyourmanager needsto makesure that it does not:

- affectyounegativelybecauseitbreaksthe WorkingTime Regulationsorhealth-and-safety regulations;
- haveanegativeeffectonyourofficialwork;or
- conflictwithyourofficialposition,orwithour interests, or damage public confidence in MoJ.

Other jobs

IfyoudoanotherjobwhilereceivingStatutory Sick Payoroccupationalsickpayfromusand are notentitledtodoso,wemaytakedisciplinary action.

Youwill notdo any otherworkwhileon special leave.

IfyouareamemberoftheSCSinHMPSin the NOMSbusinessgroup,youneedto knowthat operational grades are not allowed todo any other job without permission. See HMPS Secondary Employment Policy NTS 02/1992.

If youare not amemberof the SCS in the NOMS business group, youwillonlydootherjobsinyour owntimeandnotwhenyoushouldbeatwork.

Voluntary public service

If you are a member of the SCS in HMPS in the NOMS business group, you need to know that there are extra rules on becoming a reservist or a member of the Territorial army. You can find more details in the *Voluntary Public Service policy*.

3.13 Taking part in trade-union activities

Principle

We recognise trade unions, such as the Public and Commercial Services, FDA and Prospect. Our policy is to encourage you to join these unions.

We also provide facilities that allow our staff to take part in legitimate trade-union activities by providing reasonable time off from their normal work duties.

We have published details of the time off allowed for trade-union activities and a departmental facilities agreement, which govern the arrangements for employee representation.

All employee representatives will follow the civil service code of conduct and the facilities agreement. If you are a trade union member, you will keep to the code on *Dealing with official information* and *Political activities*.

As long as you keep to the facilities agreement, you do not need permission to promote or publish the views of your trade union on an official matter that is to do with the conditions of service of union members. However, you do need permission if your duties as an employee representative and your official work as a civil servant are in conflict.

If you comment in your role as a trade-union representative on government policy, or official matters, you will make it clear that the views are your's or those of your trade union and not that of a civil servant.

3.14 Workplace relationships

Principle

You will tell your manager about any situation where your independence or honesty may be affected, or appear to be affected, due to a close relationship with someone at work.

The aim is to avoid any possibility of problems arising. You will tell your manager as soon as possible, for example at the start of a relationship.

If you do not, your manager may take action under the disciplinary procedure.

If you are interviewing someone that you have a relationship with, as a panel member you will be asked to declare this to the chair of the panel who will decide what action, if any, to take.

You will tell your manager if your partner, close relative or friend:

- works closely to you (for example in the same management chain, or if you authorise their spending or check money they handle); or
- has connections with your workplace (for example, suppliers tendering under a procurement contract, police officers, witnesses, lawyers, defendants and prisoners).

Your manager will decide what action to take, if any, as a result of the relationship. Examples of action they could take are:

- if you manage your partner, they might decide to get someone else to carry out the performance management or appraisal role;
- to prevent you as a legal adviser from dealing with cases that involve a person close to you who may be a police officer, defence solicitor, magistrate or crown prosecutor; or
- not place you under the line management chain in the first place or to move you to another post if a relationship is likely to affect, or might be seen to affect, the honesty of the service we provide to the public.

These are examples only. Managers will assess

each case on its own merits.

3.15 Outside appointments

Principle

You may take on work when you have left the civil service as long as you follow the Business Appointment Rules for Civil Servants on getting approval, where required.

If you do not follow those rules, we may take legal action.

As a Civil Servant, or former Civil Servant, you may need to get approval **before** taking any form of full-time, reduced-hours or fee-paid employment after you have left the civil service. The rules covering whether or not you need approval are given below and apply for two years after your last day of paid service.

We do not aim to restrict you in what you do but we need to avoid any unreasonable concerns that:

- as a civil servant, you might be influenced in carrying out your official duties by the hope or expectation of future employment with a particular firm or organisation, or in a specific sector; or
- as a former civil servant, you might improperly exploit privileged access to contracts in Government or sensitive information; or
- a particular firm or organisation might gain an improper advantage by employing you who, in the course of your official duties, have had access to;
  - information relating to unannounced or proposed development in Government policy, knowledge of which may affect the prospective employer or any competitors; or
  - commercially valuable or sensitive information about any competitors.

Business Appointment Rules

Business Appointment Rules apply to all serving civil servants and to former civil servants for two years after the last day of paid service.

This includes:

- permanent civil servants;
- civil servants on fixed term contracts;
- civil servants on secondment to other organisations;
- individuals on secondment to the Civil Service from other organisations; and
- special advisers.

If any of the following apply to you, you **must** apply for approval **before** accepting any form of full-time, reduced-hours or fee-paid employment within two years after your last day of paid service.

- You are a **senior civil servant in pay band two or above**.
- You are a **special adviser.**
- You are a **senior civil servant in pay-band one or a civil servant in any grade/band below SCS** AND your circumstances match one or more of the following:
  - You have been involved in developing policy affecting your prospective employer, or have had access to unannounced Government policy or other privileged information affecting your prospective employer, at any time in your last two years in the Civil Service.
  - You have been responsible for regulatory or any other decisions, affecting your prospective employer, at any time in your last two years in the Civil Service.
  - You have had any official dealings with your prospective employer at any time in your last two years in the Civil Service.
  - You have had official dealings of a continued or repeated nature with your prospective employer at any time during your Civil Service career.

- You have had access to commercially sensitive information of competitors of your prospective employer in the course of your official duties.

- The proposed appointment or employment would involve making representations to, or lobbying the Government on behalf of a new employer.

- The proposed appointment or employment is consultancy work, either self-employed or as a member of a firm, and you have had official dealings with outside bodies or organisations in your last two years in the Civil Service that are involved in your proposed area of consultancy work.

Reporting offers of employment whilst a MoJ employee

You must report to your line manager -

- any approach from an outside employer with an offer of an appointment or employment for which approval would be required under these Rules if you plan to follow up the offer.

- **all** offers of an appointment or employment, regardless of whether or not you intend to follow them up, if you are engaged in the letting or management of Government contracts.

Special advisers should report **all** offers, to the Permanent Secretary's Office, of an appointment or employment received while they are employed as a special adviser.

Applying for approval

You should complete a business appointments application form, available on MyServices or from the HR Contact Centre and send it to Shared Services.

To ensure your application is dealt with swiftly, you must provide as much detail as possible, attaching additional sheets or documents as is necessary to answer the questions.

Who approves applications?

The application process differs dependent on your Grade – see below.

- As a **senior civil servant (pay-band 3) or above**, your application will be referred to the Advisory Committee, who provide advice to the Prime Minister, who makes the final decision. However, before submitting your application corporate Human Resources will make an initial assessment of the appointment and take an initial view on what recommendation would be appropriate.

- As a **senior civil servant (pay-bands 1 and 2)** your application will be considered by the Permanent Secretary.

- As a **special adviser**, your application will be referred to the Advisory Committee for advice but the Permanent Secretary will make the final decision based on that advice. However, before submitting your application corporate Human Resources will make an initial assessment of the appointment.

- As a **civil servant in any grade/band below SCS** your application will be dealt with by your countersigning officer's manager or relevant SCS pay-band 1, whichever is the more senior.

The Advisory Committee aims to provide its advice to the Prime Minister (or relevant Permanent Secretary in the case of applications from special advisers) within 20 working days of receipt of a fully completed application form. Complex cases may take longer, but in such cases, the Committee's Secretariat will advise the Department.

MoJ may refer any application to the Advisory Committee's Secretariat for informal advice. In addition if at any time during your last two years in the Civil Service, you have had contractual dealings with any competitors of your prospective employer, or access to information concerning them which could be regarded as commercially sensitive, the Department will seek the views of the competitors about the proposed appointment as a matter of course.

Terms ofapproval

You will be given approval either:

- unconditionally; or
- subjecttoconditionswhich mayapplyforupto two years.

Approvalwillnotnormally be givento starta paid appointment or employment with a new employerbeforecompletionofyourlastdayof paid service.

Conditions may include:

- awaitingperiodbeforetakingupthe appointment;
- a prohibitiononyou lobbying Government on behalf of your new employer;
- a condition for a specified period;
- youstandingasidefrom involvement incertain activities e.g. commercial dealings with the Department.

Any condition imposed on your appointment will runfromyour last dayofpaidservicefor uptotwo years.

Asageneralprinciple,therewillbe atwoyearban on civilservantsatSCS pay-band3 and above lobbying Government on behalf of their new employeraftertheyleavethe Civil Service. The two-yearlobbyingbanmaybereducedbythe AdvisoryCommitteeiftheyconsiderthistobe justifiedbytheparticularcircumstancesofan individual application.

For applications considered by the Advisory Committee,inadditiontoatwo-yearwaiting period,theAdvisoryCommitteemay,iftheyjudge theproprietyconcernstobesubstantial,adda ridertotheiradvicesayingthattheyalsoviewthe appointment to beunsuitable. It is for the Prime Minister(orPermanentSecretaryinthecaseof specialadvisers)to makethefinaldecisiononthe applicationbasedontheadvicereceivedfromthe Advisory Committee.

Special conditions for Permanent Secretaries

All Permanent Secretaries, including Second Permanent Secretaries, will be subject to a minimum waitingperiodofthree months between leavingpaidCivil Service employment andtaking up an outside appointmentor employment.The Advisory Committee may advise that this minimum waitingperiodshouldbewaivedif,inits judgement,noquestionsofproprietyorpublic concern arise from the appointment or employment beingtakenupearlier. Equally,the Advisory Committee may consider that public concern about a particular appointment or employment could be of such a degree or character that a longer waiting period is appropriate. Taking account of the maximum waitingperiodoftwoyearsthatmay be applied, the Committee may,exceptionally,add ariderto their advice saying that they view the appointment oremploymenttobeunsuitable.

Outcomes

Onceyourapplicationhas beenconsidered, you willbenotifiedoftheoutcome. Ifyou are asenior civilservantinpaybandtwo, theoutcome ofyour application will be copied to the Advisory Committee's Secretariat.

Where it is proposed that your application be approvedwithconditionsor awaitingperiod, you will be offered an opportunity to discuss any concernsyoumayhavewiththeofficerwhomade the decisionor withthe Advisory Committee (SCS 3 and above and special advisers).

MoJwill inform yourprospectiveemployerof any conditions which have been attached to the approvalofyour appointment or employment. For applications considered by the Advisory Committee,theiradvice,alongsidesummary detailsofyourlastpost, willusuallybepublished once you have taken up the appointment or employment or it has beenannounced.

If you wishto knowthe statusofyour application at anytimeduringtheprocess,youcancontact the HR Contact Centre.

This guidance is based on the Business Appointment Rules for Civil Servants and Guidelines for Departments on Administering the Business Appointment Rules for Civil Servants available at: http://acoba.independent.gov.uk/rules_and_guidance_civil_servants.aspx

3.16 Political activities

Principle

You will stay politically neutral at all times. You will get permission to take part in political activities if needed.

If you do not do so, your manager may take action under the disciplinary procedure.

You will serve the Government, whatever party it is formed from, to the best of your ability, no matter what your own political beliefs are. You will not act in a way that is affected by a political belief, or allow your personal political views to affect any advice you give or your actions.

You will keep to the rules governing the political activities that civil servants can be involved in. These rules are aimed at making sure that:

- ministers and the public have confidence in the independence of the civil service; and
- you are given the greatest possible freedom to take part in public affairs without affecting your duties as a civil servant.

Your senior manager will decide whether to give you permission to take part in political activities. This will depend on whether you are employed in an area where being seen as independent is at risk. You will fall into one of the following three groups, depending on your job role.

- Politically-free group – industrial and non-office (which includes drivers, ushers and messengers) staff.
- Politically-restricted group – members of the senior civil service (SCS) and civil servants at levels immediately below the SCS (band A and above), press office, legal and fast-stream employees.
- The intermediate group – employees not covered in the politically-free or restricted groups (bands B to F).

If you are not sure which group you fall into, speak to your manager.

These rules relate to activities where you might express your political views in public. They do not concern your private beliefs and opinions, prevent you from being a member of a political party or prevent you from being part of a campaign or protest group. If you want to get involved in any political activity, you may need to apply for permission. *Taking part in political activity* describes the political activities these groups can and cannot take part in, when you need permission and how to apply.

If you are a member of the SCS in HMPS, you will also have to complete a *Racial Groups and Freemasons Declaration*. You are not allowed to be a member of the British National Party, National Front, Combat 18 or any other group or organisation promoting racism. For more details see: PSO 8100, PSI 23/2000 and the Security Vetting Website.

Prison Service Orders are at: http://www.hmprisonservice.gov.uk/resourcecentre/psispsos/listpsos/

Taking part in political activity

Activities	Politically-freegroup	Politically-restricted group	Intermediate group
National political activities			
Publicannouncementasa candidate or prospective candidate for Parliament, the Scottish Parliament,the National Assembly for Wales or the European Parliament.	You are free to take part.(Youmustresign fromthecivilservicetoavoid your election beingdisqualifiedbut youwouldbeeligibletobe employedagain.)	Youcannottakepart. (You must resignfrom thecivilserviceifyou formally became a parliamentary candidate.)	Youcannottakepart. (You must resignfrom thecivilserviceifyou formally became a parliamentary candidate.)
Holdingofficeinaparty-politicalorganisation.	Youarefreetotake part.	Youcannottakepart.	Youcanapplyfor permissiontotake part.
Speakinginpublicon matters which are nationally politically controversial.	Youarefreetotake part.	Youcannottakepart.	Youcanapplyfor permissiontotake part.
Expressingviewson matters which are politically controversial in letters to thepress,intelevisionor radio broadcasts, or in booksarticlesorleaflets.	Youarefreetotake part.	Youcannottakepart.	Youcanapplyfor permissiontotake part.
Canvassing on behalf of a candidate for Parliament, the Scottish Parliament, the National Assembly for Wales or the European Parliament.	Youarefreetotake part.	Youcannottakepart.	Youcanapplyfor permissiontotake part.
Local political activities			
Beingacandidatefor,orfor co-option to, local authorities.	Youarefreetotake part.	Youcanapplyfor permissiontotake part.	Youcanapplyfor permissiontotake part.
Holdinganofficeinalocal party-political organisation.	Youarefreetotake part.	Youcanapplyfor permissiontotake part.	Youcanapplyfor permissiontotake part.
Speaking in public or expressing views, for example in letters, on matterswhicharelocally politically controversial.	Youarefreetotake part.	Youcanapplyfor permissiontotake part.	Youcanapplyfor permissiontotake part.

Activities	Politically-free group	Politically-restricted group	Intermediate group
Local political activities (*continued*)			
Canvassingonbehalfof candidatesforelectionto localauthoritiesoralocal politicalorganisation.	Youarefreetotake part.	Youcanapplyfor permissiontotake part.	Youcanapplyfor permissiontotake part.
Going to outside events.	You should not accept invitations in your official capacity to party-politicaleventsoreventsorganised by politicalpartiesorwhich couldbetodowithapolitical subjectmatter.This isbecauseit might be interpretedaslendingsupporttotheorganisationorcauseandbring our independenceintoquestion.However,ifitisinourinterestsforan official togotoaconference,forexample,as anobserver,wemaygive permission.This permission shouldbegrantedbyyourheadofdivision or areadirector.		
Unsuccessful election attempt.	You can rejoin the civil service at the same level, as long as you applywithinaweekof the day the election results are declared.	Youwillnot normally be entitled to rejoin the civil service. However, we will assess cases individually.	Youwillnot normally be entitled to rejoin the civil service. However we will assess cases individually.
Rejoiningthecivilservice afterservingasa Member of Parliament.	You are entitled to rejoin in the following circumstances. • Youstopbeingan MP after being away fromthecivil service forfiveyears orless. • Youhad at least 10 years service before youwere electedas an MP. • You apply to rejoin within three months of ending your service as an MP. We will consider all casesonmeritevenif youonly meetthefirst two of these three conditions.	You will not normally be entitled to rejoin the civil service. However, we will assess cases individually.	You will not normally be entitled to rejoin the civil service. However we will assess each case individually.

Applying for permission

Yourapplicationforpermissiontotakepartin political activitiesshould:

- be inwriting;
- give the nature of the political activity;
- givethe periodoverwhich youthinkyouwillbe involved; and
- besenttoyour areadirectoror headofdivision (or equivalent).

Whenconsideringyourapplication,yourarea directororheadofdivision(orequivalent)will considerthenatureofyourcurrentdutiesandthe type of activityyouwantpermissionfor.

We are unlikelyto giveyou permission if you carry out the followingtypes of duties.

- Ifyou are closelyinvolvedinhelping ministers with policydecisions.
- Ifyouworkin areas which arevery politically sensitiveor governed by national security.
- If you regularly speak on behalf of the Governmentorthedepartmentindealingswith commercialcompanies,pressuregroups,local government,publicauthoritiesoranyother organisation and who may appear to those organisations to influence government policy which affectsthem.
- Ifyourepresentthe Government indealings withoverseas governments.

Your responsibilities

Youwillkeeptothefollowingcodeofdiscretion if we give you permission.

- If you fall into the politically restricted and intermediate groups, you can advocate or criticise any political party. However, you shouldexpressyourcommentwithmoderation, particularlyonmattersyourownministeris responsiblefor.Youshould avoid any comment where possible if the departmental issue concerned iscontroversial.
- Avoidpersonalattacks,especiallyonyourown ministers.
- You should avoid any embarrassment to ministersortotheirdepartmentswhichcould resultfromyouractions by beinginvolved prominently in party-political controversy.
- Wegive permissionto takepartinlocalpolitical activities as longasyoudo notinvolveyourselfin matters which are politically controversial, or which areof nationalratherthanlocalsignificance.

Youwillnotcarryout any politicalactivitieswhile on duty,inuniform(ifyouwearauniform)oron officialpremises.Youwillalsocontinueto keepto therestrictionsonusingofficialinformationor experiencethatapplyto all civilservants.

What if circumstances change?

Yourareadirectorheadofdivision,(orequivalent) willreviewpermissionforpeopleto beinvolvedin politicalactivities.Youshould beawarethatwe canwithdrawpermissionto take part inpolitical activity at any time and without notice if circumstanceschange,for exampleifthenature of your work changes.

If permission is refused

We willexpectyounotto putyourselfforward prominentlyonone political sideor another.

If it isthenatureofyourcurrentrolewhichcauses theproblem,wewillconsiderthepossibilityof finding you another post.

How toappeal

If you think we have withheld permission unreasonably,youcanappealusingourgrievance procedure.

Youalso havetherighttoappealtothecivil service appeal board (CSAB).

If you want to appeal to the CSAB, you will contactthemwithineightweeksofpermission beingrefused.Youthenhaveafurtherfourweeks to sendyour casetothe CSAB. You are entitled to take a trade-union representative or work colleague to help you.

For more detailsonyoureligibility andon howto appeal, see the Civil Service appeal board's internetsite(http://www.civilserviceappealboard.gov.uk/),or contactthemon 020 72763834.

Ministry of JUSTICE

Section 04

Important intranet and access information

General information

You can get an electronic version of this policy document and related information or forms from My Services or at http://intranet.justice.gsi.gov.uk/justice/guidance-support/my-services/conduct-and-behaviour.htm

Alternative formats

If you cannot easily get access to the intranet, your manager can give you hard copy of the policy or guidance. For other formats including Braille or large print, contact the HR Contact Centre:

Email: MoJ-HR-Enquiries@NOMS.gsi.gov.uk

Phone: 0845 010 3510

Produced August 2012
Printed on paper comprising a minimum of 75% post consumer waste

Ministry
of Justice

IT Security

Policy

Contents

IT Security Policy (Overview)

This policy gives an overview of information security principles and responsibilities within the Ministry of Justice (MoJ) and provides a summary of the MoJ's related security policies and guides.

Audience

This policy is aimed at three audiences:

Technical users	These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the MoJ.
General users	All other staff working for the MoJ.

Within this policy, "all MoJ users" refers to General users, Technical users, and Service Providers as defined previously.

Associated documentation

For further guidance on IT Security, refer to the following policies.

- IT Security All Users Policy: which provides further details of the responsibilities of all MoJ users at the MoJ.
- IT Security Technical Users Policy: which provides the details of where users can find more technical and service provider related information on IT Security within the MoJ.

Principles

All MoJ users **SHALL**:

- Comply with the MoJ's Acceptable Use Policy wherever they work.
- Report all security incidents promptly and in line with MoJ's IT Incident Management Policy.
- Make themselves aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other MoJ guidance.
- Be aware of the need for Information Security as an integral part of the day to day business.
- Protect information assets under the control of the organisation.

Further information can be found in the IT Security All Users Policy.

Technical users

Technical users **SHALL** follow the guidance set out for all MoJ users in IT Security All Users Policy **AND** also comply with the IT Security Technical Users Policy.

Service Providers

Service Providers **SHALL** follow the guidance set out for all MoJ users in IT Security All Users Policy **AND** also comply with the IT Security Technical Users Policy.

Enforcement

- This policy is enforced by lower level policies, standards, procedures and guidance.
- Non-conformance with this policy could result in disciplinary action taken in accordance with the MoJ's Disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the MoJ always co-operates with the relevant authorities, and provides appropriate evidence.

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: `#security`

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for cyber security advice, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

IT Security All Users Policy

Introduction

This policy provides more information on the actions expected of all Ministry of Justice (MoJ) users when using MoJ equipment and infrastructure. It is a sub-page to the IT Security Policy Overview.

Note: In this document, the terms "data" and "information" are used interchangeably.

Audience

This policy is aimed at three audiences:

Technical users	These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the

	Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the MoJ.
General users	All other staff working for the MoJ.

Within this policy, "all MoJ users" refers to General users, Technical users, and Service Providers as defined previously.

Approach

The MoJ ensures that IT security controls are designed and implemented to protect MoJ data, IT Assets, and reputation, based around the following requirements:

Confidentiality	Knowing and ensuring that data can only be accessed by those authorised to do so.
Integrity	Knowing and ensuring the accuracy and completeness of data, and that it has not been deliberately or inadvertently modified from a previous version.
Availability	Knowing and ensuring that IT systems and data can always be accessed when required and authorised.

Assets

This policy applies to all premises, physical equipment, software and data owned or managed by the MoJ. This includes IT systems, whether developed by the MoJ or managed by IT service providers. It covers the use of IT equipment and the data processed on those IT systems, irrespective of location. It provides direction and support to preserve the confidentiality, integrity, and availability of MoJ resources.

Security classification

All MoJ Staff are responsible for ensuring data is:

- Classified correctly as detailed in the Information Classification, Handling and Security Guide
- Distributed only in accordance with the statements of this policy and related guides.
- Protected by the appropriate security controls to ensure its confidentiality, integrity and availability.

Access to classified information shall be controlled in accordance with the requirements set out within the MoJ Access Control Guide.

Physical and personnel security

The Physical Security Policy defines how physical access to assets must be controlled within the MoJ to prevent unauthorised access, use, modification, loss, or damage. All MoJ users must understand that:

- All MoJ IT systems and services must be assessed against environmental risks, for example flood or fire, to maintain the asset's confidentiality, integrity, and availability.
- The MoJ's IT Teams are not directly responsible for the physical security and environment of the MoJ sites.

- Physical security controls and the environment in which the MoJ IT systems operate form part of a system's overall risk landscape. All MoJ users **MUST** ensure they adhere to the security controls and requirements set out in this policy.
- Unless otherwise formally agreed by the MoJ, all MoJ users, including agency staff and contractors who have access to MoJ data, require Baseline Personnel Security Standard (BPSS) assessment, as a minimum.
- National Security Vetting should only be applied for where it is necessary, proportionate, and adds real value.
- The MoJ does not have a standing requirement for system administrators or application developers to maintain Security Check (SC) clearance.

Further information on physical and personnel security is available from MoJGroup Security (mojgroupsecurity@justice.gov.uk) and CPNI Guidance.

Identity and access control

The MoJ Access Control Guide ensures that information and IT assets can be accessed only by authorised personnel, and that each individual is accountable for their actions.

The guide outlines the controls and processes designed to limit access based on a "need to know" basis, and according to defined roles and responsibilities.

The MoJ Access Control Guide addresses access control principles such as identification, authentication, authorisation, and accounting.

Password management

The MoJ Password Management Guide sets out the requirements for strong password implementation and management, to help prevent unauthorised access to MoJ systems. Examples include password creation, authentication, storage and management.

Email security

The Email guidance tells you about safe and secure use of email within the MoJ.

The more detailed MoJ Email Security Guide specifies the controls and processes required to protect the MoJ's email systems from unauthorised access or misuse, that may compromise the confidentiality, integrity or availability of the data stored and shared within them.

The guide outlines the various security levels required to transfer information from the MoJ's email servers to organisations outside the MoJ and other government departments. It covers topics such as the threats to email security (phishing) and secure email transfer.

Remote working and portable devices

The MoJ has in place Remote Working guidance that sets out the requirements for safely accessing and using the MoJ's systems and applications when working remotely, for example from home, another government office, or while travelling.

Mobile computing is the use of portable equipment such as mobile phone, laptop or tablet, and which supports remote working. Mobile computing equipment provided by the MoJ must be used in line with the Acceptable Use Policy.

Any request to take MoJ IT equipment overseas must follow the guidance provided in the Acceptable Use Policy and the Accessing MoJ IT Systems From Overseas information.

Malware protection

The MoJ Malware Protection Guide specifies the controls and processes that **SHALL** be used to protect all systems against malware. Malware might enter the MoJ by employee email, through the internet, mobile computers, or removable media devices.

The MoJ Malware Protection Guide addresses the following relevant domains:

- Implementation controls to stop malware entering MoJ devices and systems.
- Preventing malicious code from executing on MoJ devices and systems.
- Mitigating the impact of malware when entering MoJ devices and systems.

Roles and responsibilities

All MoJ users are responsible for ensuring the confidentiality, integrity, and availability of data within the MoJ. This includes all MoJ data and assets. These responsibilities extend to all assets referenced in this policy.

All MoJ users **SHALL** comply with the roles and responsibilities outlined in the Information Assurance Framework Process.

Specific roles and responsibilities are described within each sub-page. All MoJ users **SHALL** comply with these roles and responsibilities, and understand these as being a part of their ultimate responsibility for information security within the MoJ.

For the purpose of this Information Security Policy, the following roles are described. They have specific responsibilities in the implementation and monitoring of different provisions of the policy.

Role	Responsibility	Which includes...
Senior Information Risk Owners (SIROs)	The MoJ SIRO is responsible for the overall MoJ information risk policy and guidance, and ensures that the policy and guidance material continues to provide appropriate risk appetite and a suitable risk framework.	Implementing and managing information risk management in their respective business groups.
		Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.
		Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.
Delegated Agency SIROs	The delegated agency SIRO is responsible for the information risk policy and guidance as it applies to their systems and personnel, and ensures the agency adheres to the MoJ's risk appetite and risk framework.	In line with the MoJ SIRO, but for Agency systems and personnel.

Role	Responsibility	Which includes...
Information Asset Owners (IAO)	IAOs, also known as IA Leads, must be satisfied that all required technical, personnel, physical and procedural security controls are in place and followed. IAOs are responsible for ensuring the management and security of their information asset over the whole asset lifecycle.	Logging and monitoring. Reviewing access permissions. Understanding and addressing risks associated to their information assets. Ensuring secure disposal of information when it is no longer required.
System Owners	System Owners are responsible for managing access control rules for their particular system.	Verifying access rights in order to assist a scheduled review audit of User accounts and permissions.
Contract Owners	Contract Owners are responsible for ensuring contractors adhere to the IT Security Policy set out here and in associated documentation.	Verify that contracts are written to reflect the MoJ's IT Security Policy. Ensure contractors comply with the requirements set out by this policy and associated documentation. Being responsible for escalating the risk of non-compliance by a supplier, and seeking guidance on suspected non-compliance with security requirements in a contract. Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the MoJ, is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: `#security`

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for cyber security advice, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.

IT Security Technical Users Policy

Introduction

This policy provides more information on the actions expected of Technical and Service Provider users when using Ministry of Justice (MoJ) equipment and infrastructure. It is a sub-page to the IT Security Policy Overview.

Audience

This policy is aimed at:

Technical users	These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.
Service Providers	Defined as any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the MoJ.

Vulnerability scanning and patch management

The MoJ Vulnerability Scanning and Patch Management Guide outlines the requirements for maintaining up to date MoJ systems and equipment to protect them from security vulnerabilities.

The guide includes patching schedules for the different MoJ systems and equipment according to their risk levels. It sets out the vulnerability ratings used to understand the criticality of a system security vulnerability. The guide addresses the following areas:

- Patching schedules and technical guides.
- Scanning requirements for different MoJ systems.

Technical controls

The MoJ Technical Security Controls Guide ensures protection from unauthorised access or misuse of the MoJ IT systems, applications, and data stored within them.

The policy outlines the control design requirements that are needed to secure the MoJ network and IT assets in accordance with the three layers of defence. The policy addresses the following areas:

- Enforcing access controls in support of the Access Control Guide.

- Building adequate security for the MoJ network and network boundaries.
- Creating secure software development and software configuration processes and designs.
- Monitoring the MoJ network against malicious code and anomalous behaviour.

Cryptography

Cryptography is a method of securing information and communication channels to allow only authorised recipients and personnel to view the information. The MoJ's IT systems **SHALL** use cryptographic technologies to provide secure connections to third party systems or to protect information "at rest" on user devices, including laptops and mobile devices.

However, where staff have procured key material or hardware through the United Kingdom Key Production Authority (UKKPA) or any other cryptographic items where National Cyber Security Centre (NCSC) dictate that national cryptographic policy applies, the NCSC dictate the policy. In this case, the Government Functional Standard - GovS 007: Security (previously HMG IA Standard No. 4, Protective Security Controls for the Handling and Management of Cryptographic Items, IS4) applies.

Note: IS4 can be accessed by joining the Cyber Security Information Sharing Partnership (CISP) and joining the UKKPA-Crpy Key Policy and Incident Management Group.

The MoJ's Staff who use cryptography **SHALL** ensure they have the appropriate level of security clearance. This requires secret (SC) level clearance for managing cryptography.

The Chief Information Security Officer (CISO) is accountable to the Senior Information Risk Owner (SIRO) and Senior Security Advisor (SSA) for ensuring the MoJ's compliance with the minimum cryptography requirements.

Software development

The MoJ ensures that all in house development, including development performed by third parties, is performed according to industry best practices and standards, as laid out in the Software Development Lifecycle Guide (SDLC).

All MoJ developers **SHALL** ensure they are aware of the importance of security when developing software and applications for MoJ use. The SDLC addresses the required methodology to be used in code development, and the security concerns that **SHALL** be accounted for during the development lifecycle.

Security incident management

The MoJ's IT Incident Management Policy covers the end-to-end incident lifecycle, and provides the guidance for the MoJ to respond effectively in the event of an IT Security Incident, which includes security incidents. Examples of topics covered are preparation for incidents, escalation and incident response, and recovery activities, including containment, resolution, and recovery.

The MoJ IT Incident Management Guide provides additional detail to the policy, but also further guidance around Incident Response Team assembly and communication channels.

Suppliers and procurement

IT Security

For the MoJ Information Assurance Framework Process to be effective, it must extend to organisations working on behalf of the MoJ or handling MoJ assets, such as contractors, offshore or nearshore managed service providers, and suppliers of IT systems. Within the Framework, the Contract owner is responsible for ensuring that:

- The supplier service delivery **SHALL** be regularly monitored, reviewed, and audited.
- When the MoJ buys IT goods, services, systems, or equipment, IT security implications **SHALL** be considered.

- All MoJ IT suppliers who handle and store information on behalf of the MoJ **SHALL** be assessed annually against the Government Functional Standard - GovS 007: Security (previously HMG Security Policy Framework) and the MoJ's IT Security Policy. Additional self-assessment requirements may be stipulated in the contract between the IT supplier and the MoJ. The MoJ's IT suppliers are responsible for carrying out these self-assessments, and for submitting those assessments to the MoJ. The MoJ is responsible for approving the assessments submitted by the supplier.
- The appropriate measures **SHALL** be put in place for any supplier not meeting compliance requirements, and the relevant MoJ teams **SHALL** be notified and consulted.
- All MoJ suppliers and contractors **SHALL** adhere to the GDPR and the Data Protection Act 2018.

Further advice can be found in the Information Classification, Handling and Security Guide.

Physical and personnel Security

The Contract owner **SHALL** include appropriate clauses in a contract with any supplier which will define the classified matter that is furnished, or which is to be developed, under said contract. This will include any relevant personnel security controls such as security clearance. Not all contracts will require such clauses, but where they are required, and failing the inclusion of this information in the contract, a separate Security Aspects Letter (SAL) is issued to the contractor along with the contract document.

Privileged users

The MoJ's Privileged User Guide sets out the key responsibilities for administrator roles within the MoJ in order to protect systems, assets and applications from unauthorised access, use, modification, or damage.

The guide sets out the security controls and processes required for the secure handling of MoJ assets and data stored and processed within them, such as the management of administrator accounts and secure configuration and change management.

Risk management

Technical risk assessment and information assurance

The MoJ risk assessment and information assurance is defined in the Information Assurance Framework Process, which requires that all IT systems that manage or are connected to government information **SHALL** be assessed to identify technical risks.

Audit

A security audit is a systematic evaluation of the MoJ's IT security management system. It is performed to maintain effective security policies and practices. These checks are subject to self or peer audit by operational line management, contract managers or MoJ HQ managers, as judged to be appropriate by the managers with responsibility for delivery. For instance, checks on Information Asset Registers and Information Risk Registers **SHOULD** be carried out quarterly, but other information assurance checks might be carried out less frequently, or triggered by events such as contract renewals.

Third party audits will be carried out by the Government Internal Audit Agency (GIAA) to provide an external evaluation of policies and practices. For more information, contact the Government Internal Audit Agency: correspondence@giaa.gov.uk

When conducting an audit:

- Documentary evidence **SHALL** be made available to auditors upon request.
- Details provided **SHOULD** include the implementation of any technical security control in an IT system. Documentary evidence of changes **SHALL** be reviewed.

- The evaluation **SHOULD** cover all types of changes, including configuration changes, to IT systems, and the IT security implications of those changes. This includes the case where no significant IT security impacts are identified.
- Evidence of operating effectiveness for technical controls **SHALL** be provided, and the desired risk mitigation as documented in the Information Assurance Framework Process.
- Activities involving verification of operational systems **SHOULD** be carefully planned and agreed to minimise disruptions to business processes.

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Operational Security Team

- Email: OperationalSecurityTeam@justice.gov.uk
- Slack: `#security`

Contact details

For any further questions relating to security, contact: security@justice.gov.uk, or for cyber security advice, contact the Cyber Assistance Team: CyberConsultancy@digital.justice.gov.uk.