



DPS Schedule 6 (Letter of Appointment Template and Order Schedules)

Letter of Appointment

This Letter of Appointment is issued in accordance with the provisions of the DPS Contract RM6124 between CCS and the Agency.

Capitalised terms and expressions used in this letter have the same meanings as in the Order Incorporated Terms unless the context otherwise requires.

ORDER:

DPS Schedule 6 (Letter of Appointment and Order Schedules)

Order Number:	██████████
From:	The Environment Agency on behalf of Defra Group
To:	Storycatchers Ltd

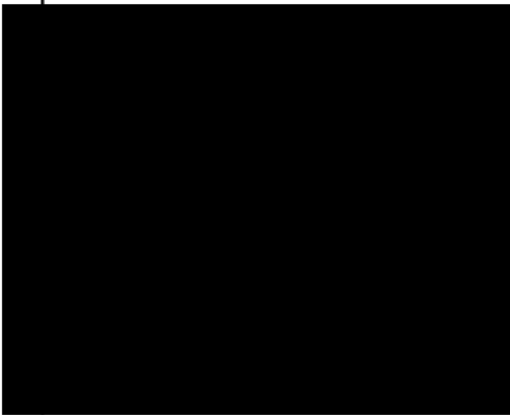
Order Start Date:	03/04/2025
Order Expiry Date:	03/07/2025
Order Initial Period:	3 months
Order Optional Extension Period:	2 month extension allowable


Goods or Services required:	<p>Goods or Services required are set out in DPS Schedule 1 of the DPS Agreement and the relevant Brief and are to be delivered in line with the accepted Proposal as detailed at Annex A of this Letter.</p> <p>Subsequent calls for Goods or Services shall be priced and agreed using the Statement of Works form as per Annex B of this Letter of Appointment.</p>
------------------------------------	--

Key Staff:	For the Customer:
	████████████████████



Department
for Environment
Food & Rural Affairs

	For the Supplier: 
Guarantor(s)	N/A

Order Contract Charges (including any applicable discount(s), but excluding VAT):	Supplier quote: £87,122.16
Liability	See Clause 11 of the Core Terms Estimated Year 1 Charges: Each Party's total aggregate liability in each Contract Year under this DPS Contract (whether in tort, contract or otherwise) is no more than £100,000
Additional Insurance Requirements	N/A
Client billing address for invoicing:	

Special Terms	N/A
----------------------	-----



Department
for Environment
Food & Rural Affairs

PROGRESS REPORT FREQUENCY

Weekly meetings to discuss ongoing progress and mitigate risks/issues.

PROGRESS MEETING FREQUENCY

Weekly meetings.

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

The rates provided on the pricing schedule

SOCIAL VALUE COMMITMENT

The Agency agrees, in providing the Goods or Services and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Proposal)

Storycatchers stated in their submission the following social value commitment: in terms of additional value delivered during the 3-month lifecycle of the project, we'd balance the need for face-to-face workshops with our sustainable 'Teams-first' travel policy and offset the carbon of any production requirements, to ensure the environmental impact of this specific project is managed.

SERVICE CREDIT CAP

N/A

ORDER INCORPORATED TERMS

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

1. This Letter of Appointment including the Order Special Terms and Order Special Schedules.
2. *Joint Schedule 1 (Definitions and Interpretation) RM6124*
3. *The following Schedules in equal order of precedence:*
 - *Joint Schedules for RM6124*
 - *Joint Schedule 3 (Insurance Requirements)*
 - *Joint schedule 2 (variation form)*
 - *Joint Schedule 4 (Commercially Sensitive Information)*
 - *Joint Schedule 11 (Processing Data)*
 - *Order Schedules for C27520*
 - *Order Schedule 6 (ICT Services)*
 - *Order Schedule 3 (Continuous improvement)*
 - *Order Schedule 7 (Key Supplier Staff)*
 - *Order Schedule 8 (Business Continuity and Disaster Recovery)]*
 - *Order Schedule 9 (Security)*
 - *Order Schedule 14 (Service Levels)*
 - *Order Schedule 15 (Order Contract Management)*
 - *Order Schedule 18 (Background Checks)*



Department
for Environment
Food & Rural Affairs

4. CCS Core Terms
5. *Joint Schedule 5 (Corporate Social Responsibility) RM6124*
6. *Order Schedule 4* (Proposal) as long as any parts of the Order Proposal that offer a better commercial position for the Client (as decided by the Client) take precedence over the documents above.

No other Agency terms are part of the Order Contract. That includes any terms written on the back of, or added to this Order Form, or presented at the time of delivery. For the avoidance of doubt, the relationship between the Parties is non-exclusive. The Client is entitled to appoint any other agency to perform services and produce goods which are the same or similar to the Goods or Services.

FORMATION OF ORDER CONTRACT

BY SIGNING AND RETURNING THIS LETTER OF APPOINTMENT (which may be done by electronic means) the Agency agrees to enter into an Order Contract with the Client to provide the Goods or Services in accordance with the terms of this letter and the Order Incorporated Terms.

The Parties hereby acknowledge and agree that they have read this letter and the Order Incorporated Terms. The Parties hereby acknowledge and agree that this Order Contract shall be formed when the Client acknowledges (which may be done by electronic means) the receipt of the signed copy of this letter from the Agency within two (2) Working Days from such receipt.



Department
for Environment
Food & Rural Affairs



Department
for Environment
Food & Rural Affairs

ANNEX A

Agency Proposal

Discover: immersing ourselves in your world [REDACTED]

We'll get moving quickly, starting our Discover process by meeting the EA team to define objectives, understand your key deliverables, and agree an approach to timings, meetings & reporting. At the same time, we'll absorb key information from you and conducting our own research, leaning on our membership of the IPA to access reports from their Insight team.

To develop and agree a plan to engage internal and external partners and stakeholders, we'll work with you to map audiences and understand who we'd need to consult. Then, we'll conduct interviews (face-to-face, online or in groups – tbc) with all available stakeholders to understand their role/relationship with the EA, their current perceptions, and views on what the new vision, mission and desired personality of the EA should include. The outputs of these meetings would then be mapped and analysed to identify barriers and opportunities for the EA, which we'd plug into a Theory of Change document to plan the process of changing perceptions, and emerging thoughts for your vision, mission and tone of voice would be grouped together thematically.

Define: exploring territories for your vision and mission – [REDACTED]

We'd use the Theory of Change document to determine the strategic notes your narrative needs to hit to change perceptions, and explore 2 or 3 of the strongest themes emerging from the stakeholder interviews, presented as visual and tonal territories for your vision and mission.

Direct: crafting the vision and mission, and outlining the narrative – [REDACTED]

With a visual and tonal territory signed off, we'd craft the first draft vision and mission statements and use them to inform the key narrative pillars and key messages of your brand story, aligned with your new 5-year strategy and our Theory of Change document. We'd also start shaping the communications plan, using the available channels and plotted against your timeframe and KPIs.

Design: creating a visual identity for the Environment Agency – [REDACTED]

Following consolidated feedback on the vision, mission and narrative, we'll brief our creative team to develop a compelling visual identity and craft long read/short drafts of your brand narrative with a supporting messaging framework. These would be applied to key comms for your approval, and then internal and external stakeholder engagement would take place.

Develop: finalising our narrative and roll out– [REDACTED]

Once the identity and messaging is approved and reflective of all stakeholder feedback, we'd create a brand guidelines document and messaging house and use it to develop a suite of communications that builds awareness and targets our key audiences in an engaging way. Budget depending, these could include videos, animations, team toolkits, leadership/HR briefing packs, e-learning materials, print assets, screen savers, newsletters, intranet / website / social content, and external comms channels where applicable.

Deliver: delivering the new narrative – [REDACTED]



Department
for Environment
Food & Rural Affairs

All assets will be prepped for launch. We'd work with you to cascade the message throughout the organisation and out into the world, followed by an evaluation and feedback phase.



Department
for Environment
Food & Rural Affairs

Annex B – Statement of work

Any schedule attached to this Statement of Work will describe in detail the different types of Services to be provided under that Statement of Work. A schedule attached to this Statement of Work only applies to the relevant project to be delivered under that Statement of Work, and not to any other Statement of Work, or to the provision of the Services as a whole.

1.1 Where a Statement of Work would result in:

- a variation of the Services procured under this Order Contract;
- an increase in the Charges agreed under this Order Contract; or
- a change in the economic balance between the Parties to the detriment of the Client that is not provided for in this Order Contract, the relevant term(s) will be dealt with as a proposed Variation to this Order Contract in accordance with the Variation procedure set out in Clause 24.

Project:

Our narrative has been defined by others; our 'brand' positioning is passive, we lack a voice and an attitude to cut through; we require a new approach to inspire our internal teams and engage external audiences. A negative reputation impacts on our ability to deliver as an organisation and to work effectively with our partners and government, it also diminishes trust with the public. By creating a clearer mission with a strong voice we can be more effective and deliver more.

Project Start date:

The start date for this project 03/04/2025 with a duration of 3 months ending 03/07/2025. There is an allowable extension of up to 2 months adhering to the variation process.

Project Notice period:

Campaign:

We require this work to happen quickly as we are currently writing our new 5-year organisation strategy that will set out our business aims and priorities. Our communications are essential to create the vision and show how we will deliver this.

Goods or Services:

We are looking for an agency who specialise in creating brand platforms for businesses and civil society organisations to enable strong communications positioning.

We are looking for creativity and expertise from an agency to help craft our narrative and mission in order to: better



Department
for Environment
Food & Rural Affairs

position ourselves; strengthen our voice with the public and media; and to enable our staff to understand and buy into this.

We are looking for the supplier to work with the organisation to create a new vision for the organisation. We want a mission statement that defines the our work, our objectives, and how we will reach these objectives.. This statement needs to reflect what we do, engage the public and our stakeholders and our staff.

We want a supporting narrative to be produced that tells our story, inspires our customers, partners, communities and our people.

The narrative needs to guide all of our communications so should focus on our language, the tone and messaging that we use to build our brand. This concise, streamlined story will act as the platform for an all of our marketing and communications - it needs to tell our story of where we have come from and where we are going. It needs to build trust with our customers and partners and show how we are delivering for the environment.

We would expect the agency to:

- Scope the work and seek initial inputs
- Agree an internal consultation process with us.
- Include proposal for external consultation with key stakeholders.

Devise plan for internal engagement and support with delivery of this

- Provide final recommendations with implementation plan

Deliverables:

- Project set up and initial inputs and agree process for internal consultation and external consultation
- External stakeholder engagement carried out
- Internal organisation engagement



Department
for Environment
Food & Rural Affairs

KPI's

- Consolidate and take on feedback
- Mission statement and organisation narrative complete:
Final recommendations report

- Regular weekly meetings will be held to agree approach, discuss any issues or revisions needed and check on timescales and deliverables.
- Relationship with supplier to be managed by Deputy Director for Communications.
- We would require Spend to Date information to be provided by the supplier at intervals agreed at the outset (likely to be weekly updates).
- We also require that relevant management information is provided to track progress against the deliverables above.

Project Plan timings:

- [REDACTED] Initial meeting to initiate the project and agree approach and deliverables would be held in [REDACTED] of supplier being appointed.
- [REDACTED] Plan for engagement with external partners and stakeholders agreed and plan for internal staff engagement agreed.
- [REDACTED] External and internal engagement delivered.
- [REDACTED] Feedback consolidated, and new narrative and mission developed.
- [REDACTED] Final report delivered - with creating of new mission statement and narrative.

Contract Charges:

The Client shall pay the Agency the sum of £87,122.16 for delivery of these Services, payable in monthly instalments. For the avoidance of doubt, the Contract Charges shall be inclusive of all third-party costs.

Client Assets:

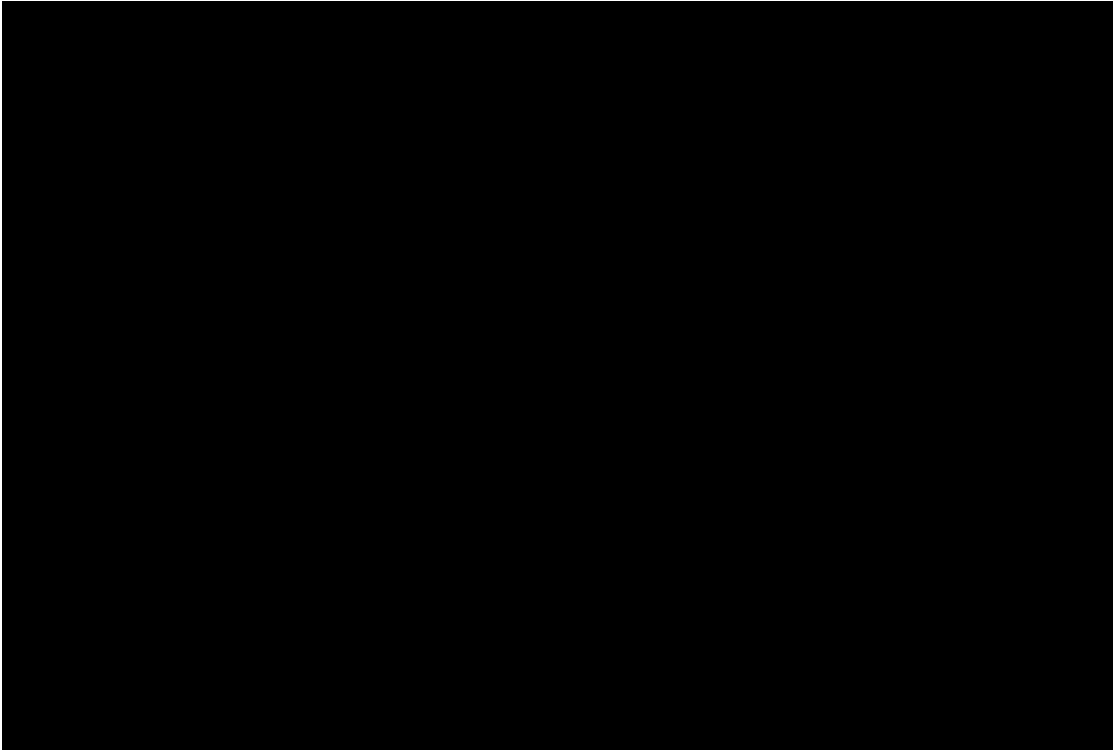
Full details will be provided In the initial scoping meetings.

International locations:

Service to be provided in the UK.



Client Affiliates	N/A
Special Terms:	N/A
Key Individuals:	
Authorised Agency Approver:	
Authorised Client Approver:	





This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details	
This variation is between:	CCS / Client ("CCS" "the Client") And Storycatchers ("the Agency")
Contract name:	Missions & Narratives ("the Contract")
Contract reference number:	DPS Contract RM6124
Details of Proposed Variation	
Variation initiated by:	
Variation number:	



Department
for Environment
Food & Rural Affairs

Date variation is raised:	
Proposed variation	
Reason for the variation:	
An Impact Assessment shall be provided within:	
Impact of Variation	
Likely impact of the proposed variation:	
Outcome of Variation	

Contract variation:	This Contract detailed above is varied as follows:	
	<ul style="list-style-type: none"> [CCS/Client to insert original Clauses or Paragraphs to be varied and the changed clause] 	
Financial variation:	Original Contract Value:	£ [insert amount]
	Additional cost due to variation:	£ [insert amount]
	New Contract value:	£ [insert amount]



Department
for Environment
Food & Rural Affairs

- 1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by [delete as applicable: CCS / Client]
- 2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
- 3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the [delete as applicable: CCS / Client]

Signature

Date

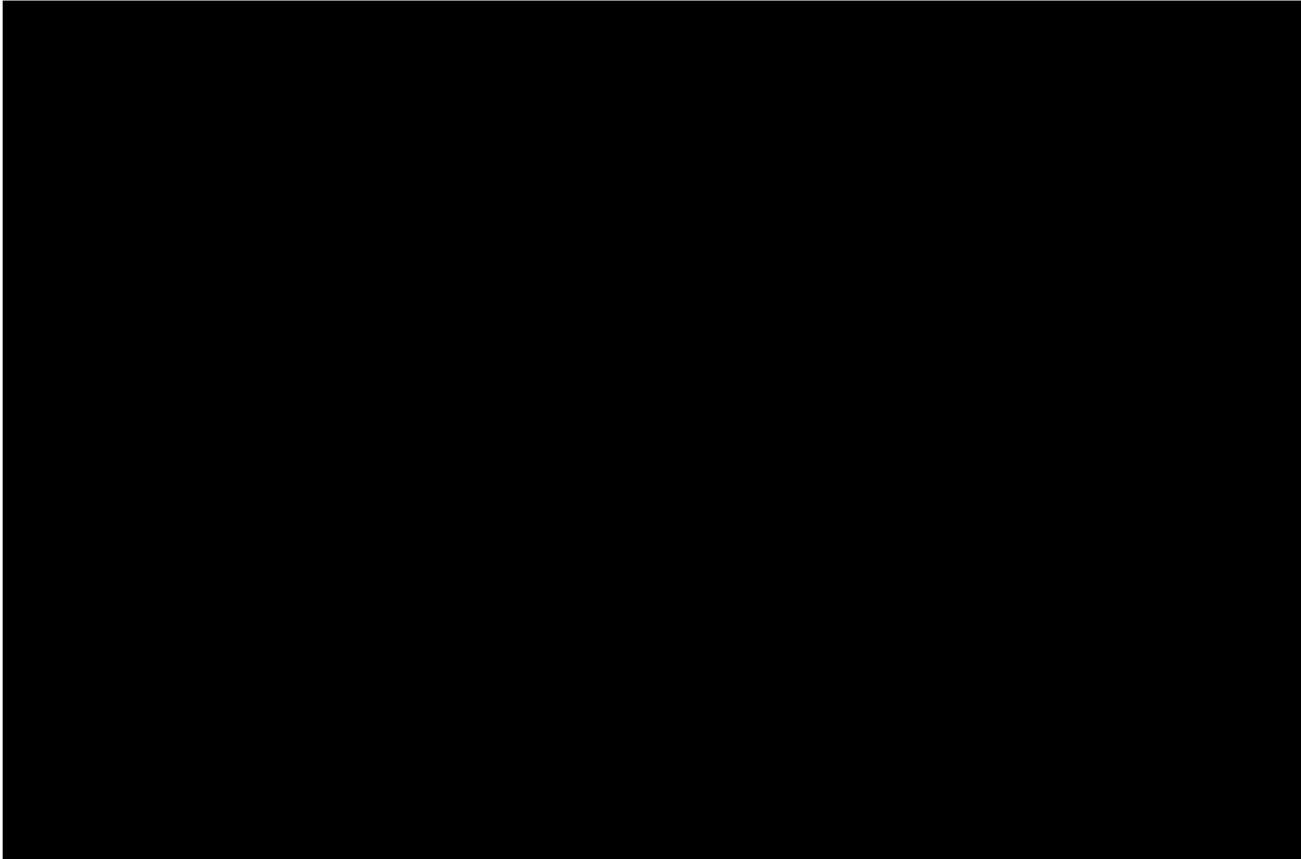
Name (in
Capitals)

Address



Department
for Environment
Food & Rural Affairs

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



Joint Schedule 5 (Corporate Social Responsibility)

1. What we expect from the Agency

- 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.



Department
for Environment
Food & Rural Affairs

(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 Agency acknowledges that the Client may have additional requirements in relation to corporate social responsibility. The Client expects that the Agency and its Subcontractors will comply with such corporate social responsibility requirements as the Client may notify to the Agency from time to time.

2. Equality and Accessibility

- 2.1 In addition to legal obligations, the Agency shall support CCS and the Client in fulfilling its Public Sector Equality duty under S149 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.



Department
for Environment
Food & Rural Affairs

3.1 The Agency:

- 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 Agency Staff or Subcontractor 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 offences 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 offences 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 Client and Modern Slavery Helpline.

4. Income Security

4.1 The Agency shall:

- 4.1.1 ensure 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 Agency Staff are 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;
- 4.1.3 ensure that all Workers are 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 Agency Staff; and
- 4.1.6 ensure that Agency Staff are engaged under a recognised employment relationship established through national law and practice.



Department
for Environment
Food & Rural Affairs

5. Working Hours

5.1 The Agency shall:

- 5.1.1 ensure that the working hours of Agency Staff comply with national laws, and any collective agreements;
- 5.1.2 Ensure that the working hours of Agency 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 is used responsibly, taking into account:

- (a) the extent;
- (b) frequency; and
- (c) hours worked;

by individuals and by the Agency Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

- 5.3.1 this is allowed by national law;
- 5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;



Department
for Environment
Food & Rural Affairs

- 5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and
- 5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Agency 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.

6. Sustainability

6.1 The Agency shall meet the applicable Government Buying Standards applicable to Goods or Services which can be found online at:

<https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>

Joint Schedule 11 (Processing Data)

Definitions

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



Department
for Environment
Food & Rural Affairs

“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

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

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

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

Where one Party is Controller and the other Party its Processor

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.

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



Department
for Environment
Food & Rural Affairs

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

- () a systematic description of the envisaged Processing and the purpose of the Processing;
- () an assessment of the necessity and proportionality of the Processing in relation to the Goods or Services;
- () an assessment of the risks to the rights and freedoms of Data Subjects; and
- () the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

- () Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
- () ensure that it has in place Protective Measures, including in the case of the Agency the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

- () nature of the data to be protected;
- () harm that might result from a Personal Data Breach;
- () state of technological development; and
- () cost of implementing any measures;



Department
for Environment
Food & Rural Affairs

() ensure that:

- () the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
- () it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

- () are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
- () are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
- () are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
- () have undergone adequate training in the use, care, protection and handling of Personal Data;

() not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

- () the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
- () the Data Subject has enforceable rights and effective legal remedies;
- () the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data



Department
for Environment
Food & Rural Affairs

that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

- () the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

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

Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

- () receives a Data Subject Access Request (or purported Data Subject Access Request);
- () receives a request to rectify, block or erase any Personal Data;
- () receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- () receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
- () receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- () becomes aware of a Personal Data Breach.

The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint



Department
for Environment
Food & Rural Affairs

Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

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

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

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

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

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



Department
for Environment
Food & Rural Affairs

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

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

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

The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

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

Where the Parties are Joint Controllers of Personal Data

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

Independent Controllers of Personal Data

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

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

Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such



Department
for Environment
Food & Rural Affairs

relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

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

The Parties shall only provide Personal Data to each other:

- () to the extent necessary to perform their respective obligations under the Contract;
- () in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
- () where it has recorded it in Annex 1 (*Processing Personal Data*).

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

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

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

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



Department
for Environment
Food & Rural Affairs

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

- () promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
- () provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

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

- () do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
- () implement any measures necessary to restore the security of any compromised Personal Data;
- () work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
- () not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

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



Department
for Environment
Food & Rural Affairs

- . Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
- . Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Agency is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 27 of this Joint Schedule 11.



Department
for Environment
Food & Rural Affairs

Annex 1 - Processing Personal Data

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

1.1.1.1 The contact details of the Relevant Authority's Data Protection Officer are: [Insert Contact details]

1.1.1.2 The contact details of the Agency's Data Protection Officer are: [Insert Contact details]

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

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

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Agency is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Agency is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> • Business email addresses • Business address
Duration of the Processing	03/04/2025 - 03/07/2025
Nature and purposes of the Processing	<i>Business Contact details of employees for contract delivery.</i>



Department
for Environment
Food & Rural Affairs

Type of Personal Data	<i>Email addresses, telephone numbers.</i>
Categories of Data Subject	<i>Staff information</i>
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	<p>Our data destruction procedure is as follows:</p> <ol style="list-style-type: none"> 1. Microsoft 365 (emails & documents) <ul style="list-style-type: none"> ○ Storycatchers' policy is that emails and any associated files containing personal data will be permanently deleted from our mailboxes 12 months after the completion of the contracted project. This allows all stakeholders time to revisit the project for clarifications or roll-on work. If you would prefer us to delete the data immediately upon completion, just let us know. ○ At the same time, any files containing personal data stored in SharePoint or OneDrive will be permanently deleted, including from the recycle bin, in line with Microsoft's data retention policies. Please note that we have policies in place to ensure email addresses are not stored anywhere other than in Outlook and Xero, to expedite this task and in order to retain project-level information divorced from personal data, for future reference. 2. Xero (financial & invoicing data) <ul style="list-style-type: none"> ○ Any personal data stored in Xero for invoicing or record-keeping will be deleted in accordance with our retention policy. This means that invoices will be retained for 6 years in accordance with HMRC guidelines. ○ After the required retention period data will be securely erased. 3. Mobile devices (telephone numbers) <ul style="list-style-type: none"> ○ Storycatchers' policy is that telephone numbers and any associated text and voice messages containing personal data will be permanently deleted from mobile devices 12 months after the completion of the contracted project. This allows all stakeholders time to revisit the project for clarifications or roll-on work. If you would prefer us to delete the data immediately upon completion, just let us know.



Department
for Environment
Food & Rural Affairs

	<ul style="list-style-type: none"> ○ Note that we forbid the use of mobile messaging services or apps (eg. WhatsApp, Signal) for project-level communication. <p>4. General data retention & deletion policy</p> <ul style="list-style-type: none"> ○ Any personal data not stored in the above systems will be manually deleted from local devices and cloud storage. Note that we have policies in place to ensure that personal data is not stored on local devices to expedite data cleansing. ○ We ensure that deleted data is not recoverable by emptying all digital recycle bins and following secure deletion practices. ○ If backups contain personal data, it will be overwritten in accordance with our backup retention policy.
--	---

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the Agency/Relevant Authority.

- () is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;
- () shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- () is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;
- () is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Goods or Services where consent is the relevant legal basis for that Processing; and
- () shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Agency's/Relevant Authority's] privacy



Department
for Environment
Food & Rural Affairs

policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

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

Undertakings of both Parties

1.1.2.1 The Agency and the Relevant Authority each undertake that they shall:

() report to the other Party every week on:

- () the volume of Data Subject Access Request (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);
- () the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- () any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
- () any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- () any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

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



Department
for Environment
Food & Rural Affairs

- () provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;
- () not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Goods or Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt, the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;
- () request from the Data Subject only the minimum information necessary to provide the Goods or Services and treat such extracted information as Confidential Information;
- () ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;
- () take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

- () are aware of and comply with their duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information;
- () are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so; and
- () have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

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



Department
for Environment
Food & Rural Affairs

- () nature of the data to be protected;
- () harm that might result from a Personal Data Breach;
- () state of technological development; and
- () cost of implementing any measures;

- () ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and
- () ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

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

Data Protection Breach

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

- () sufficient information and in a timescale, which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and
- () all reasonable assistance, including:



Department
for Environment
Food & Rural Affairs

- () co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
- () co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;
- () co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or
- () providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

1.1.3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

- () the nature of the Personal Data Breach;
- () the nature of Personal Data affected;
- () the categories and number of Data Subjects concerned;
- () the name and contact details of the Agency's Data Protection Officer or other relevant contact from whom more information may be obtained;
- () measures taken or proposed to be taken to address the Personal Data Breach; and
- () describe the likely consequences of the Personal Data Breach.



Department
for Environment
Food & Rural Affairs

Audit

1.1.4.1 The Agency shall permit:

- () the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Agency's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or
- () the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Agency so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Agency to assist in the provision of the Goods or Services.

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

Impact Assessments

1.1.5.1 The Parties shall:



Department
for Environment
Food & Rural Affairs

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

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

ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Agency amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

Liabilities for Data Protection Breach

- 1.1.7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Agency for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- () if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Agency) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant



Department
for Environment
Food & Rural Affairs

Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Agency shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Agency's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

- () if in the view of the Information Commissioner, the Agency is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Agency shall be responsible for the payment of these Financial Penalties. The Agency will provide to the Relevant Authority and its auditors, on request and at the Agency's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or
- () if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Agency shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

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

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

- () if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;
- () if the Agency is responsible for the relevant Personal Data Breach, then the Agency shall be responsible for the Claim Losses: and
- () if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Agency shall be responsible for the Claim Losses equally.



Department
for Environment
Food & Rural Affairs

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

Termination

If the Agency is in material Default under any of its obligations under this Annex 2 (*Joint Controller Agreement*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Agency in accordance with Clause 10 of the Core Terms (*Ending the contract*).

Sub-Processing

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

- () carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and
- () ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

Data Retention



Department
for Environment
Food & Rural Affairs

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

Joint Schedule 3 (Insurance Requirements)

1. THE INSURANCE YOU NEED TO HAVE

- 1.1 The Agency 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 Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Agency shall ensure that each of the Insurances is effective no later than:

- 1.1.1 the DPS 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 Order Contract Effective Date in respect of the Additional Insurances.



Department
for Environment
Food & Rural Affairs

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 at least six (6) years after the End Date.

1.3 The Agency 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 Goods or Services and for which the Agency is legally liable.

2. HOW TO MANAGE THE INSURANCE

2.1 Without limiting the other provisions of this Contract, the Agency shall:

- 2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Goods or Services 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 Agency 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.



Department
for Environment
Food & Rural Affairs

3. WHAT HAPPENS IF YOU AREN'T INSURED

- 3.1 The Agency 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 Agency 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 Agency to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Agency.

4. EVIDENCE OF INSURANCE YOU MUST PROVIDE

- 4.1 The Agency 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. MAKING SURE YOU ARE INSURED TO THE REQUIRED AMOUNT

- 5.1 The Agency 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 Agency 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 Agency 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 Agency 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 Agency 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 Agency shall promptly notify to insurers any matter arising from, or in relation to, the Goods or Services, 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 Goods or Services, the Agency 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 Agency 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 Goods or Services or this Contract on any of the



Department
for Environment
Food & Rural Affairs

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 Agency 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 Agency shall be liable for such excess or deductible. The Agency 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.



Department
for Environment
Food & Rural Affairs

ANNEX: REQUIRED INSURANCES

The Agency shall hold the following standard insurance cover from the DPS Start Date in accordance with this Schedule:

1. professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);
2. public liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than two million pounds (£1,000,000); and
3. employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) with a minimum limit of indemnity as required by Law.

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 Agency'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
1.	03/04/2025	The rates provided in the pricing schedule	Throughout the duration of the contract and once the contract expires

Order Schedule 3 (Continuous Improvement)

1. Client’s Rights

- 1.1 The Client and the Agency recognise that, where specified in DPS Schedule 4 (DPS Management), the Client may give CCS the right to enforce the Client's rights under this Schedule.



Department
for Environment
Food & Rural Affairs

2. Agency's Obligations

- 2.1 The Agency must, throughout the Contract Period, identify new or potential improvements to the provision of the Goods or Services with a view to reducing the Client's costs (including the Charges) and/or improving the quality and efficiency of the Goods or Services and their supply to the Client.
 - 2.2 The Agency must adopt a policy of continuous improvement in relation to the Goods or Services, which must include regular reviews with the Client of the Goods or Services and the way it provides them, with a view to reducing the Client's costs (including the Charges) and/or improving the quality and efficiency of the Goods or Services. The Agency and the Client must provide each other with any information relevant to meeting this objective.
 - 2.3 In addition to Paragraph 2.1, the Agency shall produce at the start of each Contract Year a plan for improving the provision of Goods or Services and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year ("**Continuous Improvement Plan**") for the Client'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 Agency or the Client and ways of working that would provide cost savings and/or enhanced benefits to the Client (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 Goods or Services including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Goods or Services; and
 - 2.3.4 measuring and reducing the sustainability impacts of the Agency's operations and supply-chains relating to the Goods or Services, and identifying opportunities to assist the Client in meeting their sustainability objectives.
-



Department
for Environment
Food & Rural Affairs

- 2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Agency to the Client 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 Client shall notify the Agency 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 Agency 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 Agency must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Agency shall provide any further information as requested.
 - 2.7 If the Client wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Agency must implement such Variation at no additional cost to the Client or CCS.
 - 2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:
 - 2.8.1 the Agency 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 Agency's progress against the Continuous Improvement Plan.
-
- 2.9 The Agency 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 Agency's costs in providing the Goods or Services to the Client be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Client by way of a consequential and immediate reduction in the Charges for the Goods or Services.
 - 2.12 If at any time during the Term the Agency reduces its DPS Prices for Goods or Services provided in accordance with the terms of the DPS Contract, the Agency shall immediately



reduce the Charges for the Goods or Services under the Order Contract by the same amount. This obligation applies whether or not the Goods or Services are offered in a catalogue provided under the DPS Contract.

Order Schedule 14 (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 Agency to the



Department
for Environment
Food & Rural Affairs

Client in respect of any failure by the Agency 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.

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

- 2.1 The Agency shall at all times provide the Goods or Services to meet or exceed the Service Level Performance Measure for each Service Level.
- 2.2 The Agency acknowledges that any Service Level Failure shall entitle the Client 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 Client as a result of the Agency's failure to meet any Service Level Performance Measure.



Department
for Environment
Food & Rural Affairs

2.3 The Agency shall send Performance Monitoring Reports to the Client 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 Client's exclusive financial remedy for a Service Level Failure except where:

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

2.4.2 the Service Level Failure:

- () exceeds the relevant Service Level Threshold;
- () has arisen due to a Prohibited Act or wilful Default by the Agency;
- () results in the corruption or loss of any Government Data; and/or
- () results in the Client being required to make a compensation payment to one or more third parties; and/or

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

2.5 Not more than once in each Contract Year, the Client may, on giving the Agency at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Agency 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;



Department
for Environment
Food & Rural Affairs

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

3. Critical Service Level Failure

3.1 On the occurrence of a Critical Service Level Failure

- 3.1.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.1.2 the Client shall be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Agency 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 Client to terminate this Contract and/or to claim damages from the Agency for material Default.



Department
for Environment
Food & Rural Affairs

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Agency:

- () is likely to or fails to meet any Service Level Performance Measure; or
- () is likely to cause or causes a Critical Service Failure to occur,

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

- 1.a.1 require the Agency to immediately take all remedial action that is reasonable to mitigate the impact on the Client and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;
- 1.a.2 instruct the Agency to comply with the Rectification Plan Process;
- 1.a.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Agency to the Client; and/or
- 1.a.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 Client shall use the Performance Monitoring Reports supplied by the Agency 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 Goods or Services and do not include VAT. The Agency shall set-off the value of any Service Credits against



Department
for Environment
Food & Rural Affairs

the appropriate invoice in accordance with the calculation formula in the Annex to Part A of this Schedule.



Department
for Environment
Food & Rural Affairs

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

Procurement-specific Service Levels should be incorporated

Service Levels			
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold
Attending weekly review meetings	Full team attendance at the weekly meetings	Any missing attendance will be noted	Attendance 100% of at least one member of the Storycatchers Ltd team
Spend data shared at the weekly review meetings and deliverable progress discussed	Clearly documented visible spend and progress on deliverables	Client able to record ongoing spend and deliverables progress weekly	Spend data and deliverable progress discussed in weekly meeting or sent via correspondence following the meeting in the scenario where not discussed in meeting.



Department
for Environment
Food & Rural Affairs

Part B: Performance Monitoring

3. Performance Monitoring and Performance Review

3.1 Within twenty (20) Working Days of the Start Date the Agency shall provide the Client with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Agency shall provide the Client with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

- 3.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
- 3.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;
- 3.2.3 details of any Critical Service Level Failures;
- 3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;
- 3.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and
- 3.2.6 such other details as the Client may reasonably require from time to time.

3.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("**Performance Review Meetings**") on a Monthly basis. The Performance Review



Department
for Environment
Food & Rural Affairs

Meetings will be the forum for the review by the Agency and the Client of the Performance Monitoring Reports. The Performance Review Meetings shall:

- 3.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Agency at such location and time (within normal business hours) as the Client shall reasonably require;
- 3.3.2 be attended by the Agency's Representative and the Client's Representative; and
- 3.3.3 be fully minuted by the Agency and the minutes will be circulated by the Agency to all attendees at the relevant meeting and also to the Client's Representative and any other recipients agreed at the relevant meeting.

3.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Agency's Representative and the Client's Representative at each meeting.

3.5 The Agency shall provide to the Client such documentation as the Client may reasonably require in order to verify the level of the performance by the Agency for any specified Service Period.

4. Satisfaction Surveys

4.1 The Client may undertake satisfaction surveys in respect of the Agency's provision of the Goods or Services. The Client shall be entitled to notify the Agency of any aspects of their performance of the provision of the Goods or Services which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.



Department
for Environment
Food & Rural Affairs

Order Schedule 15 (Order 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):

"Contract Manager"

the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Managing the contract

2.1. The Agency and the Client shall each appoint a Contract Manager for the purposes of this Contract through whom the provision of the Goods or Services shall be managed day-to-day.

2.2. The Parties shall ensure that appropriate resource and expertise is made available to deliver the aims, objectives and specific provisions of the Contract. The Client will give the Agency instructions as to its requirements for the Goods or Services. These will be included in a Statement of Work and may include start and end dates for each stage of the proposed Goods or Services.

2.3. During the Contract Period, the Agency will:

2.3.1. keep the Client fully informed as to the progress and status of all Goods or Services, by preparing and submitting written reports at such intervals and in such format as is agreed by the Parties; and

2.3.2. promptly inform the Client of any actual or anticipated problems relating to provision of the Goods or Services. Receipt of communication from the Agency by the Client



Department
for Environment
Food & Rural Affairs

does not absolve the Agency from its responsibilities, obligations or liabilities under the Contract.

-
- 2.4. During the Contract Period, the Parties' respective Contract Managers will arrange and attend meetings to review the status and progress of the Goods or Services and to seek to resolve any issues that have arisen. These meetings will be held at locations and intervals as agreed by the Parties.
- 2.5. Unless otherwise agreed in the Statement of Work, the Agency will produce contact reports providing each Party with a written record of matters of substance discussed at meetings or in telephone conversations between the parties within 3 Working Days of such discussions. If the Client does not question any of the subject matter of a contact report within 7 Working Days of its receipt, it will be taken to be a correct record of the meeting or telephone conversation.
-

3. 3. Approvals and Authority

-
- 3.1. For the purposes of this Order Schedule 15, any reference to Client Approval means written approval in one of the following ways:

-
- 3.1.1. the Client issuing a purchase order bearing the signature of an Authorised Client Approver;
 - 3.1.2. email from the individual business email address of an Authorised Client Approver;
or
 - 3.1.3. the signature of an Authorised Client Approver on the Agency's documentation.
-



Department
for Environment
Food & Rural Affairs

3.2. The Agency will seek the Client's prior Approval of:

- 3.2.1. any estimates or quotations for any costs to be paid by the Client that are not agreed in a Statement of Work; and
- 3.2.2. any creative treatments, including but not limited to scripts, messaging, storyboards, copy, layouts, design, artwork, or proposed marketing activity.

- 3.3. The Agency will seek the Client's prior Approval of any draft Goods or Services. The Client's Approval will be the Agency's authority to proceed with the use of the relevant Goods or Services.
- 3.4. If the Client does not approve of any matter requiring Approval, it must notify the Agency of its reasons for disapproval within 14 days of the Agency's request.
- 3.5. If the Client delays approving or notifying the Agency as to its disapproval, the Agency will not be liable for any resulting delays or adverse impact caused to the delivery of the Statement of Work.

4. Monitoring Campaign Performance

- 4.1. The Agency agrees to provide access to data and support for Audits undertaken by the Client and its Auditors under the CRTPA relating to campaign performance under the Contract during and after campaigns.
- 4.2. The Agency will fully comply with all remote access requests.
- 4.3. The Auditor may share data with relevant key stakeholders as necessary to complete the work. Where the Client carries out an Audit it will own the resulting report and may share non-sensitive outcomes as appropriate.
- 4.4. The Agency and the Client will agree a plan to address Audit findings to optimise campaign performance.



Department
for Environment
Food & Rural Affairs

5. Contract Risk Management

5.1. Both Parties will proactively manage risks attributed to them under the terms of this Contract.

5.2. The Agency will develop, operate, maintain and amend, as agreed with the Client, 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.

6. International Work

6.1. The management and process for Client billing under Statements of Work including international work is to be agreed prior to the commencement of the Statement of Work and set out in the Statement of Work or Letter of Appointment.



Order Schedule 6 (ICT Services)

1. Definitions

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

"Agency System"	the information and communications technology system used by the Agency in supplying the Goods or Services, including the COTS Software, the Agency Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Client System);
"Client Property"	the property, other than real property and IPR, including the Client System, any equipment issued or made available to the Agency by the Client in connection with this Contract;
"Client Software"	any software which is owned by or licensed to the Client and which is or will be used by the Agency for the purposes of providing the Goods or Services;

"Client System"

the Client's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Client or the Agency in connection with this Contract which is owned by or licensed to the Client by a third party and which interfaces with the Agency System or which is necessary for the Client to receive the Goods or Services;

"Commercial off the shelf Software" or "COTS Software"

non-customised software where the IPR may be owned and licensed either by the Agency 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:

any error, damage or defect in the manufacturing of Goods or Services; or

error or failure of code within the Software which causes Goods or Services to malfunction or to produce unintelligible or incorrect results; or

any failure of any Goods or Services to provide the performance, features and functionality specified in the requirements of the Client or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Goods



or Services from passing any Test required under this Order Contract; or

failure of any Goods or Services to operate in conjunction with or interface with any other Goods or Services in order to provide the performance, features and functionality specified in the requirements of the Client or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Goods or Services from passing any Test required under this Contract;

"Emergency Maintenance"

ad hoc and unplanned maintenance provided by the Agency 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 Client System and the Agency System;

"Licensed Software"

all and any Software licensed by or through the Agency, its Sub-Contractors or any third party to the Client for the purposes of or pursuant to this Order Contract, including any COTS Software;



Department
for Environment
Food & Rural Affairs

"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 Goods or Services by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Goods or Services 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 Client System and any premises (including the Client Premises, the Agency's premises or third party premises) from, to or at which:

oods or Services are (or are to be) provided; or
gency manages, organises or otherwise directs the provision or the use of the Goods or Services; or
any part of the Agency 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 Order Schedule shall also include any premises from, to or at which physical interface with the Client 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 Agency (or by a Sub-Contractor or other third party on behalf of the Agency) 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;

2. When this Schedule should be used



Department
for Environment
Food & Rural Affairs

- 2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Goods or Services.

3. Client due diligence requirements

- 3.1. The Agency 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 Goods or Services of the Clients 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 Agency under this Contract and/or which the Agency will require the benefit of for the provision of the Goods or Services.

- 3.2. The Agency confirms that it has advised the Client 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.

4. Licensed software warranty



Department
for Environment
Food & Rural Affairs

4.1. The Agency 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 Agency (and/or any Sub-Contractor) to the Client which are necessary for the performance of the Agency's obligations under this Contract including the receipt of the Goods or Services by the Client;

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 Order Schedule 14 (Service Levels) and Documentation; and

4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

5.1. The Agency shall:

5.1.1. ensure that the release of any new COTS Software in which the Agency owns the IPR, or upgrade to any Software in which the Agency owns the IPR complies with the interface requirements of the Client and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Client three (3) Months before the release of any new COTS Software or Upgrade;



Department
for Environment
Food & Rural Affairs

- 5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Agency 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 Agency System will be free of all encumbrances;
- 5.1.4. ensure that the Goods or Services are fully compatible with any Client Software, Client System, or otherwise used by the Agency 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 Goods or Services;

6. Standards and Quality Requirements

- 6.1. The Agency shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Goods or Services 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 Agency shall seek Approval from the Client (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 Agency of its responsibility for ensuring that the Goods or Services are provided to the standard required by this Contract.
- 6.3. Following the approval of the Quality Plans, the Agency shall provide all Goods or Services in accordance with the Quality Plans.
- 6.4. The Agency shall ensure that the Agency Personnel shall at all times during the Order Contract Period:

- 6.4.1. be appropriately experienced, qualified and trained to supply the Goods or Services 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 Goods or Services; and
- 6.4.3. obey all lawful instructions and reasonable directions of the Client (including, if so required by the Client, the ICT Policy) and provide the Goods or Services to the reasonable satisfaction of the Client.



Department
for Environment
Food & Rural Affairs

7. ICT Audit

7.1. The Agency shall allow any auditor access to the Agency 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 Agency System and pre-operational environment such as information relating to Testing;
- 7.1.3. review the Agency 's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

- 8.1. If specified by the Client in the Order Form, the Agency shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("**Maintenance Schedule**") and make it available to the Client for Approval in accordance with the timetable and instructions specified by the Client.
- 8.2. Once the Maintenance Schedule has been Approved, the Agency shall only undertake such planned maintenance (which shall be known as "**Permitted Maintenance**") in accordance with the Maintenance Schedule.
- 8.3. The Agency shall give as much notice as is reasonably practicable to the Client prior to carrying out any Emergency Maintenance.
- 8.4. The Agency 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 Goods or Services.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Agency: Specially Written Software

- 9.1.1. The Agency assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Client with full guarantee (or shall



Department
for Environment
Food & Rural Affairs

procure assignment to the Client), 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 Agency shall:

- 9.1.2.1. inform the Client 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 Client 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 Client and the Client 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 Client of any of the Agency'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 Agency hereby grants to the Client and shall procure that any relevant third party licensor shall grant to the Client a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Agency's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Client to obtain the full benefits of ownership of the Specially Written Software and New IPRs.



Department
for Environment
Food & Rural Affairs

9.1.3. The Agency 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 Client.

9.2. Licences for non-COTS IPR from the Agency and third parties to the Buyer

9.2.1. Unless the Client gives its Approval the Agency must not use any:

- 2) of its own Existing IPR that is not COTS Software;
- 3) third party software that is not COTS Software

9.2.2. Where the Client Approves the use of the Agency's Existing IPR that is not COTS Software the Agency shall grants to the Client a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Goods or Services (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Client 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 Order 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 Agency.

9.2.3. Where the Client Approves the use of third party Software that is not COTS Software the Agency shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Client on terms at least equivalent to those set



Department
for Environment
Food & Rural Affairs

out in Paragraph 9.2.2. If the Agency cannot obtain such a licence for the Client it shall:

- 9.2.3.1. notify the Client in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Agency 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 Client Approves the terms of the licence from the relevant third party.

- 9.2.4. Where the Agency is unable to provide a license to the Agency'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 Agency 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 Agency gives the Client written notice specifying the breach and requiring its remedy.

9.3. Licenses for COTS Software by the Agency and third parties to the Buyer

- 9.3.1. The Agency shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Client on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.2. Where the Agency owns the COTS Software it shall make available the COTS software to a Replacement Agency 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 Agency shall support the Replacement Agency 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.



Department
for Environment
Food & Rural Affairs

9.3.4. The Agency shall notify the Client 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. **Client's right to assign/novate licences**

9.4.1. The Client 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 Client ceases to be a Central Government Body, the successor body to the Client shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. **Licence granted by the Buyer**



Department
for Environment
Food & Rural Affairs

9.5.1. The Client grants to the Agency a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Client Software and the Specially Written Software solely to the extent necessary for providing the Goods or Services 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 Agency on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

9.6.1. Unless the Client 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 Agency shall also provide the converted format to the Buyer) into a format, which is:

- 9.6.1.1. suitable for publication by the Client as Open Source; and
- 9.6.1.2. based on Open Standards (where applicable),

and the Client may, at its sole discretion, publish the same as Open Source.

9.6.2. The Agency 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 Agency has used reasonable endeavours when developing the same to ensure that publication by the Client 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 Client System;



Department
for Environment
Food & Rural Affairs

- 9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Client 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 Client 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 Client to the Agency; and
- 9.6.2.6. do not contain any Malicious Software.

9.6.3. Where the Client has Approved a request by the Agency 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 Agency 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 Agency shall:

-
- 9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Goods or Services 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 Goods or Services 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 Goods or Services as Open Source.
-



Department
for Environment
Food & Rural Affairs

9.7. Malicious Software

- 9.7.1. The Agency 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 Goods or Services 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 Agency, where the Malicious Software originates from the Agency Software, the third party Software supplied by the Agency or the Government Data (whilst the Government Data was under the control of the Agency) unless the Agency can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Client when provided to the Agency; and
- 9.7.3.2. by the Client, if the Malicious Software originates from the Client Software or the Client Data (whilst the Client Data was under the control of the Buyer).

Agency Furnished Terms Software Licence Terms

Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in [insert reference to relevant Schedule].

Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in [insert reference to relevant Schedule].

Software as a Service Terms



Department
for Environment
Food & Rural Affairs

Additional terms for provision of a Software as a Service solution are detailed in [insert reference to relevant Schedule].

Software Support & Maintenance Terms

Additional terms for provision of Software Support & Maintenance Services are detailed in [insert reference to relevant Schedule]]

Order Schedule 7 (Key Agency Staff)

- 1.1 The Order Form (Letter of Appointment) lists the key roles ("**Key Roles**") and names of the persons who the Agency shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Agency shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Client may identify any further roles as being Key Roles and, following agreement to the same by the Agency, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Agency 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 Client or the Client 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 Agency or Subcontractor is terminated for material breach of contract by the employee.



Department
for Environment
Food & Rural Affairs

1.5 The Agency shall:

- 1.5.1 notify the Client 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 Agency 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 Goods or Services; and
- 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.

1.6 The Client may require the Agency to remove or procure that any Subcontractor shall remove any Key Staff that the Client considers in any respect unsatisfactory. The Client shall not be liable for the cost of replacing any Key Staff.



Order 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"	has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Goods or Services, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);
"Disaster Recovery Goods or Services"	the Goods or Services embodied in the processes and procedures for restoring the provision of Goods or Services following the occurrence of a Disaster;



"Disaster Recovery Plan"	has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Goods or Services following the occurrence of a Disaster;
"Related Agency"	any person who provides Goods or Services to the Client which are related to the Goods or Services from time to time;
"Review Report"	has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Agency's Proposals"	has the meaning given to it in Paragraph 6.3 of this Schedule;

2. **BCDR Plan**
- 2.1 The Client and the Agency recognise that, where specified in Schedule 4 (DPS Management), CCS shall have the right to enforce the Client's rights under this Schedule.
- 2.2 Within 10 Working Days of the Start Date the Agency shall prepare and deliver to the Client for the Client's written approval a plan (a "**BCDR Plan**"), which shall detail the processes and arrangements that the Agency shall follow to:



Department
for Environment
Food & Rural Affairs

- 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 Goods or Services; and
- 2.2.2 the recovery of the Goods or Services 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 Agency, 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 Goods or Services and any goods and/or services provided to the Client by a Related Agency;
- 3.1.3 contain an obligation upon the Agency to liaise with the Client and any Related Agencies with respect to business continuity and disaster recovery;



Department
for Environment
Food & Rural Affairs

- 3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Client and any of its other Related Agency in each case as notified to the Agency by the Client 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 Goods or Services and processes for managing those risks;
 - (c) identification of risks arising from the interaction of the provision of Goods or Services with the goods and/or services provided by a Related Agency; 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 Agency (and any Subcontractors) and for the Client;
- 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 Client 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 Client as required by the Client to inform decisions in support of the Client's business continuity plans.

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

- 3.2.1 the Goods or Services 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



Department
for Environment
Food & Rural Affairs

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 Goods or Services and the business operations supported by the provision of Goods or Services.

3.4 The Agency 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 Agency 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 Goods or Services 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 Goods or Services; and

4.1.2 the steps to be taken by the Agency upon resumption of the provision of Goods or Services 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 Goods or Services;

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 Goods or Services;

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 Goods or Services during any period of invocation of the Business Continuity Plan; and



Department
for Environment
Food & Rural Affairs

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 Agency ensures continuity of the business operations of the Client 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 Agency'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 Client Premises;
- 5.2.2 loss of utilities to the Client Premises;
- 5.2.3 loss of the Agency'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 Goods or Services during any period of invocation of the Disaster Recovery Plan;
- 5.2.11 details of how the Agency 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 Agency in relation to its obligations pursuant to this Schedule; and
- 5.2.13 testing and management arrangements.



Department
for Environment
Food & Rural Affairs

6. **Review and changing the BCDR Plan**

6.1 The Agency 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 Client 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 Agency shall conduct such reviews in accordance with the Client's written requirements. Prior to starting its review, the Agency shall provide an accurate written estimate of the total costs payable by the Client for the Client's approval. The costs of both Parties of any such additional reviews shall be met by the Client except that the Agency shall not be entitled to charge the Client for any costs that it may incur above any estimate without the Client'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 Goods or Services 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 Agency within such period as the Client shall reasonably require.
- 6.3 The Agency shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Client a report (a "**Review Report**") setting out the Agency's proposals (the "**Agency'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 Agency's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Agency's Proposals. If the Parties are unable to agree Review Report and the Agency'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 Agency shall as soon as is reasonably practicable after receiving the approval of the Agency's Proposals effect any change in its practices or procedures necessary so as to give effect to the Agency's Proposals. Any such change shall be at the Agency's expense



Department
for Environment
Food & Rural Affairs

unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Goods or Services.

7. Testing the BCDR Plan

7.1 The Agency 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 Goods or Services
- 7.1.3 at any time where the Client considers it necessary (acting in its sole discretion).

- 7.2 If the Client requires an additional test of the BCDR Plan, it shall give the Agency written notice and the Agency shall conduct the test in accordance with the Client's requirements and the relevant provisions of the BCDR Plan. The Agency's costs of the additional test shall be borne by the Client unless the BCDR Plan fails the additional test in which case the Agency's costs of that failed test shall be borne by the Agency.
- 7.3 The Agency shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Client and shall liaise with the Client in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Client.
- 7.4 The Agency shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Client. Copies of live test data used in any such testing shall be (if so required by the Client) destroyed or returned to the Client on completion of the test.



Department
for Environment
Food & Rural Affairs

7.5 The Agency shall, within twenty (20) Working Days of the conclusion of each test, provide to the Client 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 Agency's proposals for remedying any such failures.

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

8. Invoking the BCDR Plan

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

9. Circumstances beyond your control

9.1 The Agency 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.



Order 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:



Department
for Environment
Food & Rural Affairs

- () any unauthorised access to or use of the Goods or Services, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Client and/or the Agency in connection with this Contract; and/or
- () 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 Client and/or the Agency in connection with this Contract,

in either case as more particularly set out in the Security Policy where the Client has required compliance therewith in accordance with paragraph 2.2;

**"Security
Management Plan"**

the Agency's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Agency to the Client and as updated from time to time.

2. Complying with security requirements and updates to them

- 2.1 The Client and the Agency recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Client's rights under this Schedule.



Department
for Environment
Food & Rural Affairs

- 2.2 The Agency shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Client 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 Agency fully complies with the Security Policy.
- 2.3 Where the Security Policy applies the Client shall notify the Agency of any changes or proposed changes to the Security Policy.
- 2.4 If the Agency believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Goods or Services it may propose a Variation to the Client. In doing so, the Agency 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 Client pursuant to the Variation Procedure the Agency shall continue to provide the Goods or Services in accordance with its existing obligations.

3. Security Standards

- 3.1 The Agency acknowledges that the Client places great emphasis on the reliability of the performance of the Goods or Services, confidentiality, integrity and availability of information and consequently on security.
- 3.2 The Agency 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 Goods or Services and/or the Government Data; and
- 3.2.4 where specified by the Client in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.



Department
for Environment
Food & Rural Affairs

- 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 Agency from time to time.
- 3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Agency should notify the Client's Representative of such inconsistency immediately upon becoming aware of the same, and the Client's Representative shall, as soon as practicable, advise the Agency which provision the Agency shall be required to comply with.

4. Security Management Plan

4.1 Introduction

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



Department
for Environment
Food & Rural Affairs

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 Agency;
- c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Client with access to the Goods or Services, processes associated with the provision of the Goods or Services, the Client Premises, the Sites and any ICT, Information and data (including the Client'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 Goods or Services;
- d) be developed to protect all aspects of the Goods or Services and all processes associated with the provision of the Goods or Services, including the Client Premises, the Sites, and any ICT, Information and data (including the Client's Confidential Information and the Government Data) to the extent used by the Client or the Agency 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 Goods or Services;
- e) set out the security measures to be implemented and maintained by the Agency in relation to all aspects of the Goods or Services 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 Goods or Services comply with the provisions of this Contract;
- f) set out the plans for transitioning all security arrangements and responsibilities for the Agency 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 Agency and the Client engaged in the provision of the Goods or



Department
for Environment
Food & Rural Affairs

Services 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 Agency shall prepare and deliver to the Client 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 Client 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 Agency shall amend it within ten (10) Working Days of a notice of non-approval from the Client and re-submit to the Client 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 Client. If the Client 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 Client 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 Client 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 Client 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 Agency of its obligations under this Schedule.
-



Department
for Environment
Food & Rural Affairs

4.4 **Amendment of the Security Management Plan**

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

- a) emerging changes in Good Industry Practice;
- b) any change or proposed change to the Goods or Services 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 Client.

4.4.2 The Agency shall provide the Client 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 Client. 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 Agency proposes to make to the Security Management Plan (as a result of a review carried



Department
for Environment
Food & Rural Affairs

out in accordance with Paragraph 4.4.1, a request by the Client or otherwise) shall be subject to the Variation Procedure.

- 4.4.4 The Client 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 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 Agency shall:
- 5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Client) 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 Client 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 Client, where the Client 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 Client.



Department
for Environment
Food & Rural Affairs

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 Client.

Security Policy

1 Table of Contents

- 1 Table of Contents 2
- 2 Change control..... 3
 - 2.1 Document Control Statement..... 3
 - 2.1.1 Access Guidelines..... 3
 - 2.1.2 Handling and Disposal Guidelines..... 3
 - 2.1.3 Communications Guidelines..... 4
- 3 Definitions 4
- 4 Overview 4
- 5 Purpose..... 4
- 6 Scope..... 5
- 7 Applicability 5
- 8 Policy Statements 6
 - Physical and Environmental Security 6
 - Asset and Software Registers..... 7
 - Information Assurance 9
 - Business Continuity 10
 - Personnel Security..... 11
 - Third Party Service Providers 11
- 9 Compliance, Governance and Monitoring 12
- 10 Exceptions..... 13
- 11 Supporting Documentation 13



2 Change control

2.1 Document Control Statement

The following outlines the access, handling, communication and disposal guidelines that apply to this document.

2.1.1 Access Guidelines

There are no restrictions on internal Defra Group employee access to this document, or to contractors/consultants, third parties and any other agency or body with access to Defra Group assets or data handling facilities.

2.1.2 Handling and Disposal Guidelines

To be handled and disposed of in accordance with the Government Security Classification procedures for OFFICIAL information.



Department
for Environment
Food & Rural Affairs

2.1.3 Communications Guidelines

All Defra Group security policies must be communicated within the organisations and be available to interested parties, as appropriate. Care should be taken not to disclose sensitive information and must be produced in protected PDF format.

3 Definitions

- “Defra Group” includes the core Department and Delivery Partners;
- “Defra Departmental Security Officer” refers to the senior security officer, who is responsible for overall Defra-wide.

4 Overview

- 4.1 Defra Group has a number of business assets, including buildings, physical items, ICT services and systems, information and personnel, all of which have a high value to the Department and therefore need to be suitably protected.
- 4.2 This policy has been developed to ensure an adequate level of protection for these business assets from a wide range of threats and events which may jeopardise Defra Group activities. Defra Group employs a risk management approach to the implementation of physical, procedural, technical and personnel security controls across the Department. This ensures that all risks pertinent to Defra Group’s business assets are identified, prioritised and managed in an effective and consistent manner, thereby maintaining their confidentiality, integrity and availability, as appropriate.

5 Purpose

- 5.1 This document forms the Security Policy for Defra Group and is a statement of the Department’s commitment to establish and maintain the security and confidentiality of information, information systems, applications, network and physical assets and buildings owned or held by Defra Group by:
 - 5.1.1 Achieving a secure and confidential working environment;
 - 5.1.2 Ensuring the availability of systems and information to authorised individuals;
 - 5.1.3 Ensuring compliance with legal, regulatory and contractual requirements;
 - 5.1.4 creating and maintaining within Defra Group a level of awareness of the need for Information, Physical and Personnel Security as an integral part of the day to day business, by ensuring that Defra Group employees are aware of and fully comply with applicable legislation as described in this and the relevant security policies maintained by the Defra Group;
 - 5.1.5 Maintaining the reputation and operation of Defra Group in the eyes of the Department’s customers, end-users and stakeholders;



Department
for Environment
Food & Rural Affairs

5.1.6 ensuring there is a consistent level of security for Defra Group information assets to ensure the confidentiality, integrity and availability is maintained, whilst minimizing the risk of compromise from unauthorised disclosure and access, thereby ensuring data quality is preserved;

5.1.7 Ensuring breaches of information security and suspected weaknesses are reported and investigated;

5.1.8 Ensuring Business Continuity and Disaster Recovery plans are established, maintained and tested.

This policy applies to all information held in both physical and electronic form.

5.2 Legal requirements

Some aspects of information security are governed by legislation, the most notable UK acts are;

- The General Data Protection Act (2018)
- Computer Misuse Act (1990)
- Regulation of Investigatory Power Act (2000)
- Freedom of Information Act (2000)

6 Scope

6.1 The scope of this policy applies to:

6.1.3 All Defra Group staff, contractors, temporary staff and external third party suppliers who require logical or physical access to Defra Group information systems or premises;

6.1.4 To all colleagues, contractors/consultants, contractual third parties and any other agency or body with access to Defra Group information, information assets, IT equipment or data handling facilities.

7 Applicability

7.1 This Defra Group Security Policy applies to:

7.1.1 All Defra Group employees, including Civil Servants, Defra Group system users, casuals, consultants and contractors and visitors who have access to Defra Group business assets, who are responsible for reading and implementing the measures described within this policy and affording the appropriate level of protection to Defra Group's business assets;

7.1.2 All systems, products, services and processes owned or commissioned by Defra Group or acquired from an external supplier, including Cloud Based Infrastructure managed by Defra Group employees, security issues must be considered throughout their life-cycle, from inception through to de-commissioning;

7.1.3 All Defra Group locations from which Defra Group systems are accessed (including home use or other remote use). Where there are links to enable non-Defra Groups (to have access to Defra Group information) Defra Group must confirm the security



Department
for Environment
Food & Rural Affairs

policies they operate to meet the Defra Group security requirements set out in this policy and the risks are understood and mitigated.

8 Policy Statements

Physical and Environmental Security

Physical and Environmental security measures must be implemented to prevent unauthorised physical access, damage and interference to the Defra Group buildings.

8.1 It is the policy of Defra Group to ensure that:

- 8.1.1 Physical and Environmental controls are enforced at all locations where Defra Group information, physical or personnel assets or systems maintain a presence, in order to prevent the unauthorised access, modification, loss or destruction of business assets;
- 8.1.2 A layered approach to physical security is taken, combined with an approach to ensure that all measures are commensurate with the asset(s) being protected;
- 8.1.3 The physical measures enforced will prevent, deter, delay and/or detect, attempted or actual unauthorised access, acts of damage and/or violence being conducted towards Defra Group business assets;
- 8.1.4 Access to Defra Group premises, information data and information systems will be limited to authorised personnel only. Authorisation will be demonstrated through the use of authorisation credentials by common access control pass / security pass that have been issued by Defra Group;
 - 8.1.4.1 Passes must be visibly displayed at all times, whilst on Defra Group premises to demonstrate authorisation, and removed when leaving Defra Group premises;
 - 8.1.4.2 Passes are official documents. The unauthorised possession, use, retention, alteration, destruction or transfer to another person is an offence. The loss of this pass must be reported to the issuing authority immediately.
- 8.1.5 In the event that visitors need access to the Defra Group premises, information data or information systems, those visitors must have prior authorisation, must be positively identified, and must have their authorisation verified before physical access is granted. Once access has been granted, visitors must be escorted and their activities monitored at all times;
- 8.1.6 Physical assets must be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access;
- 8.1.7 Equipment used to handle, store, transmit and process Defra Group data must be correctly maintained and protected from power failures and other disruption caused by failures in supporting utilities, to ensure its continued availability;



Department
for Environment
Food & Rural Affairs

- 8.1.8 Physical access control measures are implemented and tested to ensure they are fit for purpose and offer the required protection;
- 8.1.9 Critical, sensitive or security classified business assets will be located in a secure area within a defined security perimeter protected by appropriate level of physical controls, determined by associated risks;
- 8.1.10 all networked file servers/central network equipment will be located in secure areas with restricted access, confined to designated employees whose job function requires access to that particular area/equipment.

Asset and Software Registers

8.2 Equipment Inventory

- 7.2.1 Defra Group assets associated with information and information processing facilities must be identified and an inventory of these assets must be maintained.

8.3 ICT Security

It is the policy of Defra Group to ensure that:

- 8.3.1 All Defra Group systems are subject to a risk assessment, and must be performed when the system processes or holds personal data, the risk management approach will be appropriate and decided by Defra Group Security.

All Defra Group systems and infrastructure will be considered for scope within IT Security Health Checks at least annually, or as required on any major system change, to ensure that the technical implementation of the system is secure and compliant with Defra Group policies;

- 8.3.2 The technical measures applied to Defra Group systems are to be consistent with the requirements outlined in each system risk assessment. As a minimum, the following measures will be applied:

- 8.3.2.1 All Defra Group systems will employ identification and authentication controls to enable the management of user accounts, manage the need-to-know requirement and manage the risk of unauthorised access;

- 8.3.2.2 All Defra Group ICT equipment, including laptops, desktop PCs, servers, Mobile Devices and Defra Group hardware (e.g. Defra Group appliances, firewalls, routers, hubs and switches) that processes Defra Group information and systems will be locked down in accordance with accepted best practice to restrict services and ensure the need-to-know requirement is implemented. The term "locked down" refers to the secure configuration of the device/system in order to minimise risks from misuse, which may compromise the integrity, confidentiality and availability of the information being processed by or stored on the device;

- 8.3.2.3 Measures must be in place to ensure that the latest vulnerabilities and threats that have the potential to affect Defra Group systems and its infrastructure can be identified, assessed and acted upon accordingly;



Department
for Environment
Food & Rural Affairs

- 8.3.2.4 All Defra Group systems and tools provided will be appropriately patched and kept up to date to fix known issues or security weaknesses throughout the lifetime of the product to reduce the risk from known vulnerabilities;
 - 8.3.2.5 Defra Group systems and all associated infrastructure will have a protective monitoring policy applied that is in line with HMG policy, and as a minimum, ensures that any breach of the confidentiality, integrity and availability of that system and its information assets can be reliably and quickly detected and that the integrity of the audit trail is ensured;
 - 8.3.2.6 There will be effective configuration management through a formal change control and asset management process, where all changes to ICT systems/applications will be subjected to a security impact assessment;
 - 8.3.2.7 Measures must be in place to protect Defra Group's business assets from modification, damage or loss due to malicious software, including viruses, spyware and phishing;
 - 8.3.2.8 Measures must be in place to ensure that Defra Group communications facilities (including the use of Email, Internet and Intranet) are used in an efficient, effective, ethical and lawful manner and in accordance to the PSN CoCo requirements.
- 8.3.3 All Defra Group systems will employ boundary security devices, where appropriate, to ensure protection from untrusted Organisations.
- 8.3.4 The use of removable media is not permitted except when the conditions below are met:
- Seek permission where necessary from the relevant IAO, especially if it concerns personal data, sensitive information;
 - minimise their use;
 - only use them where there is a good business reason;
 - always use the most appropriate and secure type of removable media;
 - Apply encryption for sensitive information or personal data if it must be saved to removable media.
- 8.3.5 Where a removable device/medium is used, it must be owned or issued on behalf of the Department and only used for Departmental business purposes. Media containing information must be protected against unauthorised access, misuse or corruption where possible.
- 8.3.6 Use of personally owned devices/media to hold or carry Defra Group information or connect to Defra Group systems is not permitted under any circumstances.
- 8.3.7 Defra Group-approved removable media devices should not be connected to non-Defra Group systems or personally owned devices unless explicit prior authorisation has been given. This includes Defra provided BlackBerrys and smartphones.
- 8.3.8 Where removable media is received from outside the Department the recipient must be expecting it, must have adequate assurances that it has been scanned for malicious content, and it must be for business, not personal use.



Department
for Environment
Food & Rural Affairs

- 8.3.9 Users must not use Defra Group provided/approved devices to download data or information that contravenes the Acceptable Use Policy.
- 8.3.10 Users are formally made aware that it is a breach of security to download files which disable the network or which have the purpose of compromising the integrity and security of Defra Group file servers or to intentionally introduce files which cause system disruption could be prosecutable under the Misuse of Computer Act 1990.
- 8.3.11 Defra Group systems must have a formal registration and de-registration process in place to control access. Periodic review of user access rights must be undertaken, including those with privileged access rights.

Defra Group employees, contractors and temporary staff working for the Department and its delivery partners must only access systems for which they are authorized.

Information Assurance

8.4 It is the policy of Defra Group to ensure that:

- 8.4.1 There is a consistent level of security for all Defra Group information assets, thereby minimising the risk of compromising their confidentiality, integrity and availability. In particular:
 - 8.4.1.2 The confidentiality of information and other business assets is maintained, by protecting Defra Group's information assets from unauthorised disclosure and unauthorised access;
 - 8.4.1.3 The integrity of information and data quality is preserved, by ensuring that it is accurate, up to date and complete;
 - 8.4.1.4 The availability of information assets, systems and services to authorised users is maintained.
- 8.4.2 All employees, contractors and temporary staff working for the Department and its delivery partners must be made aware of their duty to safeguard the Confidentiality, Integrity and Availability of the information that they store, handle or process.
- 8.4.3 All security related risks to Defra Group information assets will be managed in accordance with Defra Group's Information Risk Policy.
- 8.4.4 A whole-life, systematic and layered approach of technical, procedural, personnel and physical security measures is implemented to ensure the protection of end-user information (in particular personal and sensitive personal information as defined by the UK Data Protection Act 2018) and Defra Group information assets from unauthorised access or disclosure. All Defra Group business assets must be protected in line with the Government Security Classifications scheme.
- 8.4.5 All media devices holding personal data and/or sensitive material must be encrypted.
- 8.4.6 All information assets and business assets used to store personal data and/or sensitive material, must be securely disposed of in accordance with HMG IA Standard No.5 when no longer required.



Department
for Environment
Food & Rural Affairs

- 8.4.7 All information assets and business assets used to store personal and/or sensitive data must not be left unattended and will be appropriately secured when not in use in line with the Defra Group Clear Desk and Clear Screen Policy.
- 8.4.8 Access to information assets that are subject to the 'need-to-know' principle will be restricted to authorised personnel who have the need to know that information to fulfil their role.
- 8.4.9 Incident Management procedures must be established to ensure that all breaches or suspected breaches of ICT, Information Security, physical assets and information loss are reported (if necessary, anonymously), recorded, investigated and mitigated quickly and effectively. Incident Management procedures must outline reporting requirements in the event the incident impacts Data Protection Act, PSN etc. A cultural change programme must be undertaken to raise awareness amongst all Defra Group, contractors and third party staff of the relevant security policies and procedures adopted by Defra Group.
- 8.4.10 Information security education and training must take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.
- 8.4.11 A data retention policy is established and enforced (with exception to RPA) to ensure compliance to statute and the UK Data Protection Act 2018.
- 8.4.12 All contractual, regulatory and legislative requirements are met, to ensure that Defra Group and its Delivery Partners retain their organisational status, as appropriate e.g. Paying Agency accreditation status.
- 8.4.13 All risks associated with the sharing of Defra Group information assets are reviewed, managed and authorised by the relevant Information Asset Owner, thereby ensuring that information is only used within the law for public good.

Business Continuity

8.5 It is the policy of Defra Group to ensure that:

- 8.5.1 Business Continuity plans (BCP) and Disaster Recovery (DR) plans are produced, maintained and exercised for Defra Group's business assets, to minimise damage and ensure that Defra Group's business operation can be effectively recovered/restored in the event of a major failure or disaster;
- 8.5.2 Employees are aware of the existence of the plans and their specific responsibilities in the event of a disaster and BCP or DR plans being invoked;
- 8.5.3 BCP and DR plans are formally reviewed as required and as a minimum on an annual basis, by the relevant business area to ensure they are up-to-date and fit for purpose.

The complete Business Continuity Policy can be located [here](#).



Department
for Environment
Food & Rural Affairs

Personnel Security

8.6 It is the policy of Defra Group to ensure that:

- 8.6.1 Personnel controls are applied to all Defra Group employees, contractors and visitors;
- 8.6.2 The identities of all employees, contractors and temporary staff working for the Department are assured, in terms of their trustworthiness, integrity and reliability;
- 8.6.3 The level of clearance required for each employee and/or contractor with access to Defra Group business assets is determined on a case by case basis according to the role being fulfilled. As a minimum, all personnel must be subject to the Baseline Personnel Security Standard (BPSS) before the commencement of employment. Full implementation of BPSS, including a 100% application of 'unspent' criminal record check, is explicitly mandated as part of the security policy framework;
- 8.6.4 Defra Group/Delivery Partners shall ensure all new employees are made aware of their security responsibilities as part of their induction;
- 8.6.5 Defra Group/Delivery Partners shall ensure that staff are made aware of their responsibility to report any behaviours of security concern relating to colleagues or visitors.

Third Party Service Providers

8.7 It is the policy of Defra Group to ensure that:

- 8.7.1 All Service Providers are responsible for complying with Defra Group's Security Policy, and all associated security policies and procedures.
- 8.7.2 All Service Providers are responsible for ensuring that all Service Provider employees or contractors, who require access to Defra Group's business assets, are subject to the Baseline Personnel Security Standard as a minimum, before access is granted.
- 8.7.3 No access will be granted to any of Defra Group networks without formal authority.
- 8.7.4 Documentary evidence is obtained from all Service Providers on a yearly basis, to demonstrate compliance with established and agreed Defra Group's policies and procedures.
- 8.7.5 Defra Group will regularly monitor, review and audit Service Providers to gain assurance of compliancy to regulatory and legal requirements, including adherence to Defra Group policies and procedures.



Department
for Environment
Food & Rural Affairs

9 Compliance, Governance and Monitoring

9.1 Compliance will be governed by the following Policy and standards:

9.1.1 HMG Security Policy Framework

9.1.2 ISO/IEC 27001:2013

9.2 In order to ensure compliance with these policies, Defra Group reserves the right to:

9.2.1 Monitor the use of Defra Group systems, respond to concerns regarding alleged or actual violations of this policy; and, if necessary, take appropriate action;

9.2.2 Monitor and record access to Defra Group sites and premises using monitoring and access control systems;

9.2.3 Monitor Defra Group's electronic communication systems and to enforce policies relating to the use of electronic information and those communication systems;

9.2.4 Access an individual's account, with the exception of the designated locations used to store personal information, via the electronic systems, including when that individual is not available;

9.2.5 Conduct compliance visits and audits against Defra Group policies and procedures to ensure they are being conformed too;

9.2.6 Consideration of ITHC when new systems are developed, upgraded or when significant changes occur;

9.2.7 Co-operate fully with any police enquiry or other lawful enquiry into alleged illegality arising as a result of prohibited use, recognising that this may assist in the criminal prosecution of any Defra Group employee(s) involved.

9.3 Non-compliance with this policy or other Defra Group security policies, unless by prior arrangement with Defra Group SSA, will be reported to the relevant delivery partners Security Risk Owner. Where the minimum requirements of the Security Policy Framework are not met in full, or are adapted, Defra Group will inform the Cabinet Office in writing.

9.4 All employees are responsible for information security and therefore must understand and comply with this policy and the supporting policies available. It is the duty of each employee who uses or has access to information to be aware of, and abide by, the policies and arrangements concerning the secure use and protection of Defra Group Assets.

It is the responsibility of each Line Manager to ensure that all employees who they are responsible for are trained and supported in information security requirements. It is the responsibility of DEFRA Group to provide employees with the necessary guidance, awareness and, where appropriate, training in relation to all applications, systems and Organisations they have access to; and employees will adhere to and abide by the rules controlling applications, systems and Organisations.

All personnel or suppliers providing a service for Defra and the Defra Group have a duty to:

- Safeguard hardware, software and information in their care;

DPS Schedule 6 (Letter of Appointment and Order Schedules)

Crown Copyright 2021

- Prevent the introduction of malicious software on the Defra Group's information systems;
- Report any suspected or actual breaches in security.

All managers are directly responsible for implementing the policy and ensuring employees compliance within their respective departments.

Failure to observe or comply with the standards set out in this policy may be regarded as gross misconduct and any breach may render an employee liable to disciplinary action under the Defra Group or Local Delivery Partners disciplinary procedures, which may result in dismissal.

Third party contractors/consultants and any other agency or body accessing Defra Group assets or data handling facilities must have disciplinary procedures in place to cover breaches to the Defra Group's Security Policies by their employees.

10 Exceptions

Compliance to the principles within this policy is mandatory for all staff, contractors and third party suppliers and they are set to protect both the information assets we have and the systems that hold them. Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or increase costs. These will need to be risk assessed on a case by case basis. Where there are justifiable reasons why a particular Policy requirement cannot be implemented, a policy exception may be requested to the local security representative. Exceptions may be granted to an individual, a team/group or a service area or Directorate and may be for a temporary period or on a permanent basis, but subject to review.

11 Supporting Documentation

All other Defra Group Security Policies support this overarching document.

- Security Policy Framework.
- Government Security Classification scheme
- ISO/IEC27001:2013
- CESG Good Practice Guides (GPG)

HMG Information Assurance documentation