Framework Schedule 6 (Direct Award short order form template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	**con_3910**
THE BUYER: **Technology (DSIT)**	**Department of Science, Innovation and**
BUYER ADDRESS	1 Victoria Street, London, SW1H 0ET
THE SUPPLIER:	**Saxton Bampfylde**
SUPPLIER ADDRESS:	9 Savoy Street, London, WC2E 7EG
REGISTRATION NUMBER:	RM6290
DUNS NUMBER:	297550360

This Order Form, when completed and executed by both Parties, forms a Call-Off Contract. A Call-Off Contract can be completed and executed using an equivalent document or electronic purchase order system.

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 21 March 2023.

It's issued under the Framework Contract with the reference number RM6290 for the provision of Executive & Non Executive Recruitment Services.

CALL-OFF LOT:

- Lot 2 Executive Search - SCS3 & SCS4 (and equivalents)

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

1. This Order Form
2. Joint Schedule 1(Definitions and Interpretation) **RM6290**
3. The following Schedules in equal order of precedence:

- Joint Schedules for **RM6290**
    - Joint Schedule 2 (Variation Form)
    - Joint Schedule 3 (Insurance Requirements)
    - Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 5 (Corporate Social Responsibility)
    - Joint Schedule 11 (Processing Data)

- Call-Off Schedules for **RM6290**
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.11)
5. Joint Schedule 5 (Corporate Social Responsibility) **RM6290**

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF START DATE: **23/03/2023**

CALL-OFF EXPIRY DATE: **23/03/2024**

GDPR POSITION
Independent Controller (default unless specified); or Controller to Processor; or Joint Controller

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

CALL-OFF DELIVERABLES

Executive search support to recruit to the role of National Technology Adviser (SCS PB3), Department of Science, Innovation and Technology

Redacted Under s43(2) of the FOIA

CALL-OFF CHARGES
£42,000

PAYMENT METHOD
Redacted under s43(2) of the FOIA

BUYER'S INVOICE ADDRESS:
1 Victoria Street
London
SW1H 0ET

BUYER'S AUTHORISED REPRESENTATIVE
Redacted under s40(1) of the FOIA

SUPPLIER'S AUTHORISED REPRESENTATIVE
Redacted under s40(1) of the FOIA

SUPPLIER'S CONTRACT MANAGER
Redacted under s40(1) of the FOIA

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

Joint Schedule 2 (Variation Form)

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

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

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

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

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

Joint Schedule 3 (Insurance Requirements)

1. **The insurance you need to have**

1. The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:
    1. the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and
    2. the Call-Off Contract Effective Date in respect of the Additional Insurances.
2. The Insurances shall be:
    1. maintained in accordance with Good Industry Practice;
    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;
    3. taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and
    4. maintained for at least six (6) years after the End Date.
3. The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2. **How to manage the insurance**

1. Without limiting the other provisions of this Contract, the Supplier shall:
    1. take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;
    2. promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and
    3. hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3. **What happens if you aren't insured**

1. The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

2. Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4. **Evidence of insurance you must provide**

1. The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5. **Making sure you are insured to the required amount**

1. The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. **Cancelled Insurance**

1. The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

2. The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

1. The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

2. Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

3. Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

4. Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the Framework 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 five million pounds (£5,000,000); and
   3. employers' liability insurance [with cover (for a single event or a series of related events and in the aggregate) of not less than] five million pounds (£5,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

1. **What is the Commercially Sensitive Information?**

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

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).

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.			
2.			
3.			

Joint Schedule 5 (Corporate Social Responsibility)

1. **What we expect from our Suppliers**
   1. In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)
   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.
   3. The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.
2. **Equality and Accessibility**
   1. In addition to legal obligations, the Supplier shall support CCS and the Buyer 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:
      1. eliminate discrimination, harassment or victimisation of any kind; and
      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.

1. The Supplier:
   1. shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;
   2. shall not require any Supplier 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. warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.
   4. warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.
   5. shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world.

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;
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;
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;
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;
10. shall not use or allow child or slave labour to be used by its Subcontractors;
11. shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4. **Income Security**
   1. The Supplier shall:
      1. ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
      2. ensure that all Supplier 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;
      3. 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. record all disciplinary measures taken against Supplier Staff; and
      5. ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5. **Working Hours**
   1. The Supplier shall:
      1. ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;
      2. that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

3. ensure that use of overtime used responsibly, taking into account:
    a. the extent;
    b. frequency; and
    c. hours worked;

by individuals and by the Supplier Staff as a whole;

2. The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
3. Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
    1. this is allowed by national law;
    2. this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

appropriate safeguards are taken to protect the workers' health and safety; and

    3. the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

4. All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

2. **Sustainability**
    1. The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs

Joint Schedule 11 (Processing Data)

Definitions

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

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

Status of the Controller

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

a. "Controller" in respect of the other Party who is "Processor";
b. "Processor" in respect of the other Party who is "Controller";
c. "Joint Controller" with the other Party;
d. "Independent Controller" of the Personal Data where the other Party is also "Controller",

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

Where one Party is Controller and the other Party its Processor

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

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

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

a. a systematic description of the envisaged Processing and the purpose of the Processing;
b. an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
c. an assessment of the risks to the rights and freedoms of Data Subjects; and
d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

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

approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

i. nature of the data to be protected;
ii. harm that might result from a Personal Data Breach;
iii. state of technological development; and
iv. cost of implementing any measures;

c. ensure that :

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

A. are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;

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

C. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

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

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

i. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
ii. the Data Subject has enforceable rights and effective legal remedies;
iii. the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
iv. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

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

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

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

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

9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
a. the Controller with full details and copies of the complaint, communication or request;
b. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
c. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
d. assistance as requested by the Controller following any Personal Data Breach; and/or
e. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
a. the Controller determines that the Processing is not occasional;
b. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
c. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

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

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

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

b. obtain the written consent of the Controller;

c. enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

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

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

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

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

Where the Parties are Joint Controllers of Personal Data

17. 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

18. 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.

19. 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.

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

21. 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.

22. The Parties shall only provide Personal Data to each other:

a. to the extent necessary to perform their respective obligations under the Contract;

b. 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

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

23. 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.

24. 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.

25. 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")**:

a. 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

b. 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:

i. 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

ii. 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.

26. 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:

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

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

c. 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

d. 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.

27. 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).*

28. 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)*.

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

Annex 1 - Processing Personal Data

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

1. The contact details of the Relevant Authority's Data Protection Officer are:
2. The contact details of the Supplier's Data Protection Officer are: DSIT Data Protection Officer, Department for Science, Innovation & Technology, 1 Victoria Street, London SW1H 0ET. Email: dataprotection@beis.gov.uk.
3. The Processor shall comply with any further written instructions with respect to Processing by the Controller.
4. Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: • Name of Candidate(s), employment history, qualifications, right to work and security clearances and personal data to undertake compliance checks. • Business contact details of Supplier and key contacts **The Supplier is Controller and the Relevant Authority is Processor** *The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 3 to paragraph 16 of the following Personal Data:* • ***[Insert** the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier]*

	The Parties are Joint Controllers *The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:* • ***[Insert** the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together]* **The Parties are Independent Controllers of Personal Data** *The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:* • *Business contact details of Supplier Personnel for which the Supplier is the Controller,* • *Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,* • ***[Insert** the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority]*
Duration of the Processing	From award until expiry of all Call Off Contracts under RM6290.
Nature and purposes of the Processing	Managing the obligations under the Framework Agreement, including exit management, and other associated activities. This information may be shared with the Authority to enable compliance checks on the Supplier to be undertaken. This information will be shared digitally in a secure manner.

Type of Personal Data	***All Data Subjects*** *As following, but not limited to:* *Full name, Workplace address, Workplace Phone Number, Workplace email address, Names, Job Title, Compensation, Tenure Information, Qualifications or Certifications, Nationality, Education & training history, Previous work history, Personal Interests, References and referee details, Driving license details, National insurance number, Bank statements, Utility bills, Job title or role* *Job application details, Start date, End date & reason for termination, Contract type, Compensation data, Photographic Facial Image, Biometric data, Birth certificates, IP Address, Details of physical and psychological health or medical condition* *Next of kin & emergency contact details, Record of absence, time tracking & annual leave*
Categories of Data Subject	Data Subjects may include: ● Staff (employees) and Contracted Employee ● Self Employed Contractors ● Customers/Clients ● Suppliers
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	The Supplier must retain and store securely any data in relation to a Call Off Contract for a minimum of 7 years after the expiry of the agreement. Once this period has ended the Supplier must destroy any data stored in line with 10.5 of the Core Terms.

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 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 18-28 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 supplier:

a. 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;

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

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

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

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

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

2. **Undertakings of both Parties**

1. The Supplier and the Relevant Authority each undertake that they shall:

a. report to the other Party every 3 months on:

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

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

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

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

v. any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

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

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

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

d. not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Deliverables 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;

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

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

g. 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:

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

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

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

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

i. nature of the data to be protected;

ii. harm that might result from a Personal Data Breach;

iii. state of technological development; and

iv. cost of implementing any measures;

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

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

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

3. **Data Protection Breach**

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:

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

b. all reasonable assistance, including:

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

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

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

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

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:

a. the nature of the Personal Data Breach;

b. the nature of Personal Data affected;

c. the categories and number of Data Subjects concerned;

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

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

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

4. **Audit**

1. The Supplier shall permit:

a. 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 Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

b. the 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 Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Deliverables.

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

5. **Impact Assessments**

1. The Parties shall:

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

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

6. **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 Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. **Liabilities for Data Protection Breach**

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

a. if in the view of the Information Commissioner, the 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 Supplier) 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 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 Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

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

c. if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

2. If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("Court") by a third party

in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

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

a. if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

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

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

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

8. **Termination**

If the Supplier 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 Supplier in accordance with Clause 10 of the Core Terms (*Ending the contract*).

9. **Sub-Processing**

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

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

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

10. **Data Retention**

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

Call-Off Schedule 5 (Pricing Details)

Firm price - £42,000

Payment profile:

Redacted under s43(2) of the FOIA

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

Executive search support to recruit to the role of National Technology Adviser (SCS PB3), Department of Science, Innovation and Technology

Redacted under s43(2) of the FOIA

<u>Executive search service requirements</u>

Redacted under s43(2) of the FOIA