This Order Form is for the provision of the Call-Off Deliverables. It is issued under the Framework Contract RM6160: Non Clinical Temporary and Fixed Term Staff.

Contracting Authority Name	UK Research and Innovation (UKRI)
Contracting Authority Contact	[redacted]
Contracting Authority Address	Polaris House, North Star Avenue, Swindon, SN2 1FL
Invoice Address (if different)	N/A

Supplier Name	LA International Computer Consultants Limited
Supplier Contact	[redacted]
Supplier Address	Festival Way, Stoke-on-Trent ST1 5UB

Framework Ref	RM6160: Non Clinical Temporary and Fixed Term Staff
Framework Lot	3
Call-Off (Order) Ref	GSS23540
Order Date	26/06/2023
Call off Start Date	03/07/2023
Call-Off Expiry Date	31/12//2023
Extension Options	N/A
GDPR Position	Independent Controller
Number of roles required:	1
Number of CV's required:	0
Job role / Title	Technical Delivery Manager
Temporary or Fixed Term Assignment	Temporary
Hours / Days required	Full time – [redacted] hours per week / Maximum [redacted] working days
Unsocial hours required – give details	N/A
High cost area supplement details	None
Immunisation requirements? (Fee type 1 only)	N/A

Pay band	10A	
Fee Type	Non-Patient Facing (No Disclosure)	
Expenses to be paid or benefits offered	Expenses shall be paid in alignment with the UKRI Travel Policy	
Expenses to be paid by Temporary Worker	No	
Charge rates	Pre-AWR	Post-AWR
	£[redacted]/Day)	£[redacted] (/Day)
	[redacted] Working Days @ £[redacted] ex VAT = £78,611.40 exc VAT The contract shall not exceed £78,611.40 exc. VAT	

	It is the viewpoint of the contracting authorities that the candidate above is in scope of the intermediaries' legislation (IR35). All workers are subject to 28 calendar days' notice period.
Method of payment	The supplier shall issue electronic invoices weekly in arrears following customer approval of the workers timesheet. The customer shall pay the supplier within thirty (30) calendar days upon receipt and acceptance of a valid invoice. Invoice to include purchase order number and contract reference shall be sent to [redacted]
Discounts applicable	N/A

Criminal records check	N/A
BPSS required	Yes
State required clearance and background checking	N/A
Skills, mandatory training and qualifications necessary for the role	As a PM / Delivery Manager you will support and deliver several projects within the Information Security Programme. These are mainly governance-based activities and you will work on the following activities: - The delivery of a review of the information security policy documents that exist across UKRI. - The creation of an Architecture led Information Security roadmap - The delivery of an internal cyber assessment framework review - The delivery of a discovery of Privileged Access Management for UKRI You will need to work effectively collaborating across internal and external multi-functional teams to deliver the above activities, on time and to the desired cost and quality. You will need experience of the following: - Delivery of governance projects for Information Security - Experience working with several teams and third parties - Delivery of a cyber assessment framework or similar activity And will involve: - Creation of project plans and keeping stakeholders to account to deliver any required inputs on time. - Creation of project initiation documents, benefit realisation mapping documents etc. - Identification and Management of Risks, issues, assumptions and dependencies. - Ability to summarise project progress effectively and to talk through with senior stakeholders

	- Working largely in isolation, so a persistent, self starter mentality is required • This role will best suit an individual who enjoys working as part of a team, is well organised, pragmatic, with a technical mind and delivery focus

CALL-OFF INCORPORATED TERMS

The Call-Off Contract, Core Terms and Joint Schedules' for this Framework Contract are available on the CCS website. Visit the Non Clinical Temporary and Fixed Term Staff web page and click the 'Documents' tab to view and download these.

CALL-OFF DELIVERABLES

The requirement
The requirements to be delivered by the Supplier to the Contracting Authority in accordance with the Framework Specification during the specified Call-Off Period For further details about what can and cannot be included here please email - info@crowncommercial.gov.uk

PERFORMANCE OF THE DELIVERABLES

Key Staff
[redacted]
Key Subcontractors
N/A

For and on behalf of the Supplier:		**For and on behalf of the Contracting Authority:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Role:	Managing Director	Role:	Head of Procurement
Date:	30/06/2023	Date:	30/06/23

Joint Schedule 11 (Processing Data)

1 Status of the Controller

1. 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. 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 there 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.

2 Where one Party is Controller and the other Party its Processor

2. 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.

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

4. 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 Services;

(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.

5. 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 promptly 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 Data Loss Event;

(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*);

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(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 arefulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with 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

Contract Ref: GSS23540

copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

6. 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:

(a) receives a Data Subject Request (or purported Data Subject 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 Data Loss Event.

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

8. Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable 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 Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly 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 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 Data Loss Event; 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.

9. 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 GDPR or Personal Data relating to criminal

Contract Ref: GSS23540

convictions and offences referred to in Article 10 of the GDPR; or

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

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

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

12. Before allowing any Sub-processor 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.

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

14. The Relevant Authority may, at any time on not less than 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).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 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.

3 Where the Parties are Joint Controllers of Personal Data

16. 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 GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

4 Independent Controllers of Personal Data

17. 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.

18. 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

Contract Ref: GSS23540

be in breach of it.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 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 reasonablyrequire.

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

21. 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 GDPR); and

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

22. 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 GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

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

24. 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 ofreceipt of the request or correspondence, inform the other Party that it has

Contract Ref: GSS23540

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.

25. 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.

26. 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)*.

27. 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)*.

28.

Notwithstanding the general application of paragraphs 2 to 15 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 paragraphs16 to 27 of this Joint

Contract Ref: GSS23540

5 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 contract details of the Customer Data Protection Officer is [redacted]

2. The contract details of the Suppliers Data Protection Officer is [redacted]

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

3. Any such further instructions shall be incorporated into this Schedule.

Contract Reference	**GSS23540**
Date	**Monday 26th June 2023**
Description of Authorised Processing	**Details**
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation the Parties are Independent Controllers of Personal Data under this Framework Agreement.
Use of Personal Data	Managing the obligations under the Call Off Contract Agreement, including exit management, and other associated activities.
Duration of the processing	For the duration of the Framework Contract plus 7 years.
Nature and purposes of the processing	The nature of the processing will include collection, organisation, structuring, storage, alteration, retrieval, consultation, use, restriction, erasure or destruction of data. Erasure will be by manual means. Processing takes place for the purposes of:

Contract Ref: GSS23540

	• Pre-employment checking The nature of processing will include the storage and use of names and business contact details of staff of both the Contracting Authority and the Supplier as necessary to deliver the Services and to undertake Contract and performance management. The Contract itself will include the names and business contact details of staff of both the Contracting Authority and the Supplier involved in managing the Contract.
Type of Personal Data	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 Ref: GSS23540

	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	Agency worker/s of the contracting authority as engaged by the supplier. Staff of the Contracting Authority and the Supplier, including where those employees are named within the Contract itself or involved within contract management.