

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

Order Form

CALL-OFF REFERENCE: C234138

THE BUYER: The Secretary of State for Health and Social Care acting as part of the Crown.

BUYER ADDRESS 39 Victoria Street, London, SW1H 0EU

THE SUPPLIER: Burges Salmon LLP

SUPPLIER ADDRESS: 1 Glass Wharf, Bristol, BS2 0ZX

REGISTRATION NUMBER: OC307212

DUNS NUMBER: XXXXXXXXXX

SID4GOV ID: 432710

This Order Form is for the provision of the Call-Off Deliverables and dated 25/01/2024 It's issued under the Framework Contract with the reference number Legal Services Panel RM6179 for the provision of legal advice and services.

CALL-OFF LOT(S):
Lot 1 – General Legal Advice and Services

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

Crown Copyright 2018

CALL-OFF INCORPORATED TERMS

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

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6179
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
 - Joint Schedules for RM6179
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 6 (Key Subcontractors)
 - Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Call-Off Schedules for C234138
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 2 (Staff Transfer)
 - Call-Off Schedule 3 (Continuous Improvement)
 - Call-Off Schedule 5 (Pricing Details)
 - Call-Off Schedule 20 (Call-Off Specification)
 - Call-Off Schedule 24 (Special Schedule)
5. CCS Core Terms (version 3.0.11)
6. Joint Schedule 5 (Corporate Social Responsibility) RM6179

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

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

Where the Services provided under the Call-Off Contract include Legal Services and **Schedule 24 (Special Schedule) Legal Services Contract** applies, in addition to the amendments set out in Schedule 24, the following amendments shall be deemed incorporated into Schedule 24:

4. Pricing and Payments

4.12 Buyer (client) monies

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

Crown Copyright 2018

- (a) The Supplier shall deposit Buyer monies with such banks as the Supplier may from time to time decide in accordance with its regulators' Accounts Rules.
- (b) The Supplier has no immediate control over these monies while they are held on deposit and the Supplier will not be liable to the Buyer for any monies lost as a result of the failure of the bank. In these circumstances, the Buyer may be entitled to compensation under the Financial Services Compensation Scheme.
- (c) Interest is earned on the Supplier's Client Account. The Supplier has an interest rate policy which is designed to ensure the Buyer is treated fairly and which complies with the Supplier's regulatory requirements. This policy is available on request.

34. Resolving Disputes

Complaint Handling

34.10 The Supplier's complaints handling procedure can be viewed here: <https://www.burges-salmon.com/contact-us/complaints-handling-procedure>.

34.11 The Supplier is not authorised by the Financial Conduct Authority (FCA). The Supplier is, however, included on the register maintained by the FCA so that it can carry on insurance distribution activity, which is broadly the advising on, selling and administration of insurance contracts. This part of the Supplier's business is regulated by the Solicitors Regulation Authority and arrangements for complaints or redress are subject to the jurisdiction of the Legal Ombudsman. The register can be accessed at www.fca.org.uk/firms/financialservices-register.

CALL-OFF START DATE: 18/03/2024.

CALL-OFF EXPIRY DATE: 13/03/2026.

CALL-OFF INITIAL PERIOD: 2 years. An option to extend for a further year.

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification).

The Buyer is entitled to 2 hours of free initial consultation and legal advice with each Order in accordance with Paragraph 5.2 of Framework Schedule 1 (Specification).

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

Crown Copyright 2018

MANAGEMENT OF CONFLICT OF INTEREST

None so far as the Supplier (confirmed in conflict-of-interest declaration for tender dated 25/01/2024) and Customer are aware.

CONFIDENTIALITY

Nothing additional to the CCS Core Terms

IPR

Nothing additional to the CCS Core Terms

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms, and as amended by the Framework Special Terms (Lot 1).

For the purposes of Clause 11.2 of the Core Terms (as amended by the Framework Special Terms), the Supplier's liability for any damages, costs, claims, expenses, interest or other liability arising out of the performance or non-performance by the Supplier (or by any person for whom the Supplier may be liable vicariously) of its obligations under this Call-Off Contract (whether by virtue of negligence or otherwise) shall be limited to £3 million per claim. When considering what may be regarded as one claim for the purposes of this limit of liability all claims against the Supplier arising from one act or omission, one series of related acts or omissions, the same act or omission in a series of related matters or transactions, similar acts or omissions in a series of related matters or transactions and all claims against the Supplier arising from one matter or transaction will be regarded as one claim.

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

VOLUME DISCOUNTS

Where the Supplier provides Volume Discounts, the applicable percentage discount (set out in Table 2 of Annex 1 of Framework Schedule 3 (Framework Prices)) shall automatically be applied by the Supplier to all Charges it invoices regarding the Deliverables on and from the date and time when the applicable Volume Discount threshold is met and in accordance with Paragraphs 8, 9 and 10 of Framework Schedule 3.

REIMBURSABLE EXPENSES

Recoverable as stated in the Framework Contract, in line with DHSC travel and expenses policy (including reasonable subsistence for hearings).

DISBURSEMENTS

Payable – Subject to prior approval being obtained before incurred.

WORK\49897461\v.1

Framework Ref: RM6179

Project Version: v1.0

Model Version: v3.7

ADDITIONAL TRAINING CHARGE

N/A

SECONDMENT CHARGE

N/A

PAYMENT METHOD

Payment of undisputed invoices will be made within 30 days of receipt of invoice, which must be submitted promptly by the Supplier, to the following details.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

BUYER'S INVOICING ADDRESS:

All invoices must be sent, quoting a valid Purchase Order Number (PO Number) and any other relevant details, to: [REDACTED]

BUYER'S AUTHORISED REPRESENTATIVE

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

BUYER'S ENVIRONMENTAL POLICY

Available Upon Request

BUYER'S SECURITY POLICY

Available Upon Request

BUYER'S ICT POLICY

Available Upon Request

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

SUPPLIER'S CONTRACT MANAGER

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

SUBCONTRACTOR'S AUTHORISED REPRESENTATIVE

[REDACTED]
[REDACTED]
[REDACTED]

PROGRESS REPORT

As advised by chair to the Inquiry.

PROGRESS MEETINGS AND PROGRESS MEETING FREQUENCY

As advised by the Chair to the Inquiry.

KEY STAFF

[REDACTED]
[REDACTED]
[REDACTED]

KEY SUBCONTRACTOR(S)

[REDACTED]

COMMERCIALLY SENSITIVE INFORMATION

Call Off Schedule 5 (Pricing details)

SERVICE CREDITS

Not applicable

ADDITIONAL INSURANCES

Not Applicable

GUARANTEE

Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in tender dated 25/01/2024.

Framework Schedule 6 (Order Form Template and Call-Off Schedules)
Crown Copyright 2018

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:	[REDACTED]	Signature:	[REDACTED]
Name:	[REDACTED]	Name:	[REDACTED]
Role:	[REDACTED] [REDACTED]	Role:	[REDACTED] [REDACTED] [REDACTED]
Date:	15 March 2024	Date:	19/03/2024

Call-Off Schedule 20 (Call-Off Specification)

1. THE REQUIREMENT

1.1 To provide a Solicitor to the Inquiry and a wider team to fulfil the following items including the below. This is not an exhaustive list and is likely to develop further as the Inquiry progresses.

1.1.1 Key personnel – the supplier’s team will include a Partner or Senior Solicitor to fulfil the role of Solicitor to the Inquiry. That individual should remain in the Solicitor to the Inquiry role throughout the duration of the contract.

- 1.1.1.1 The Solicitor to the Inquiry will need to demonstrate strong leadership, communication and organisational skills and the ability to work flexibly and at pace.
- 1.1.1.2 They should have strong legal skills, an excellent knowledge of the Inquiries Act 2005 and Inquiry Rules 2006, and the ability to work both independently and as part of a multi-disciplinary team.
- 1.1.1.3 The post holder should have excellent drafting and analytical skills and be able to take a proactive approach to problem solving, dealing with novel and unpredictable challenges.
- 1.1.1.4 Given the nature of this Inquiry, the solicitor to the Inquiry should be able to demonstrate a proven track record of dealing with victims and families of victims of unlawful killings– and their lawyers, and have experience and expertise in dealing with the police when a criminal investigation is running alongside an inquiry.

1.1.2 Advice on Investigative strategy – the Supplier will provide advice to the Chair on the investigative approach to enable successful, efficient, and timely delivery of the Inquiry’s Terms of Reference, including (but not limited to):

- 1.1.2.1 Providing advice to the Chair on the segmentation of the Inquiry’s Terms of Reference, including potential topics for public hearings
- 1.1.2.2 Scheduling of hearings, taking evidence
- 1.1.2.3 Requesting evidence from organisations and individuals and analysing that evidence for relevance.
- 1.1.2.4 Analysis of evidence, and advice on the provision of expert evidence and selection of witnesses, including providing advice on anonymity issues or restriction orders.
- 1.1.2.5 Overseeing the implementation of redactions to material to be disclosed to Core Participants.
- 1.1.2.6 Management of the disclosure process.
- 1.1.2.7 Identifying witnesses for public hearings and taking witness statements from relevant organisations and individuals, in the event that the witness is unrepresented.
- 1.1.2.8 The structure and delivery of Inquiry reports.

1.1.3 Coordinate the work of the Inquiry's wider Legal Team:

- 1.1.3.1 Working with Counsel to the Inquiry in the management of the Counsel team in a way which best allocates resources to each topic the Inquiry intends to cover, ensuring that there is sufficient drafting capacity on each team, and that work is conducted at the appropriate level.
- 1.1.3.2 Oversight of work across the wider Inquiry Legal Team, ensuring that duties are divided appropriately between Counsel, Solicitors and Paralegals, and that work is conducted at the most cost effective level.
- 1.1.3.3 Working with Counsel to the Inquiry and the Inquiry Secretariat to plan the resources required in the Inquiry Counsel and Paralegal teams. This may include the Supplier providing paralegals to work on the Inquiry.

1.1.4 Inquiry procedures – the Supplier will be responsible for the legal elements of delivery of the Inquiry's operation, including (but not limited to)

- 1.1.4.1 Developing and overseeing procedures for evidence management and disclosure
- 1.1.4.2 Advice and direction on applications for Core Participant status, and management of the interactions with Core Participants during the Inquiry's work. The Supplier should forge productive relationships with Core Participants and their legal representatives.
- 1.1.4.3 Advising the Chair on funding applications made under Section 40 of the Inquiries Act 2005. This will include liaising with Core Participants and their legal representatives, monitoring actual spending against awarded funds, for which a costs draughtsman or dedicated solicitor will be required reporting costs to the Inquiry Secretary before payment;
- 1.1.4.4 Advice on data protection, data breaches and any communication with the Information Commissioner's Office, to include provision of a Data Protection Officer, if required.
- 1.1.4.5 Advice on the management and delivery of Inquiry public hearings, ensuring that hearings run smoothly.
- 1.1.4.6 Advice on the legal implications of other areas of the Inquiry's work – for example commissioning research.
- 1.1.4.7 The Supplier will also work with the Inquiry Secretariat to plan and manage resources for the Inquiry Counsel and Paralegal teams. This may include providing paralegals to supplement the Inquiry's team on occasions.
- 1.1.4.8 Providing legal advice on other ad-hoc aspects of the Inquiry's work where appropriate – for example, providing advice on the Inquiry's safeguarding responsibilities, responses to correspondence and media enquiries, and advising on website policies and content.

1.1.5 The supplier will work closely with the Inquiry secretariat to ensure that all legal work is delivered within budget and with value for money in mind. The supplier will be responsible for:

- 1.1.5.1 Management of the overall spend, including the oversight of the cost of counsel, solicitors and paralegals, achieving efficiency and value for money, keeping the cost within forecasted limits, working closely with the secretariat to ensure that spend is accurately reported.

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

Crown Copyright 2018

- 1.1.5.2 Notifying the Authority at the earliest opportunity of any potential overspend against budget forecast. The supplier will discuss with the Authority any work, instruction or resourcing change which may have a financial impact to the Authority.
- 1.1.5.3 Ensuring that work is undertaken by counsel, solicitors and paralegals with the appropriate and necessary experience, with consideration to value for money throughout – for example, ensuring that a more junior counsel (at a lower fee) is instructed for work when it is appropriate to do.
- 1.1.5.4 Providing cost draughtsmen support to the processing of s.40 invoices and ensuring that s.40 awards to Core Participants offer value for money.
- 1.1.6 Providing legal advice to the Inquiry Secretariat as necessary** on the management and collation of documentation including the **maintenance of the Inquiry record**, the provision and management of virtual data and/or e-disclosure as well as hard copy records management, and any legal support needed facilitating the transfer of the inquiry record to the appropriate public record office;
- 1.1.7 The supplier will instruct and manage relationships with experts. The Inquiry will require the supplier to:**
 - 1.1.7.1 Identify and develop, in collaboration with the Chair, Counsel and Secretary to the Inquiry, the specification and instructions for expert witnesses.
- 1.1.8 The supplier may on occasion provide contingency for hearings staff. The Inquiry may require the supplier to:**
 - 1.1.8.1 Source appropriate security, on advice from the secretariat to inquiry hearings or at other Inquiry events which require additional security.
 - 1.1.8.2 Source other staff for hearings if considered appropriate by the Secretariat, including but not limited to a hearings manager, ushers and AV support.
- 1.1.9 The Supplier will assist with the production of Inquiry reports, including but not limited to:**
 - 1.1.9.1 Working with the Counsel team and the Inquiry Secretariat to advise the Chair on potential findings and recommendations they may wish to make arising from the Inquiry's investigations.
 - 1.1.9.2 Working with the Inquiry's communications personnel to establish and maintain a consistent 'house style' for Inquiry reports.
 - 1.1.9.3 Quality assuring Inquiry reports to ensure that, for example, references to the Inquiry's evidence base are accurately recorded.
 - 1.1.9.4 Management of the 'Maxwellisation' process to ensure that all parties criticised in draft reports have the opportunity to respond prior to publication.
 - 1.1.9.5 On occasion, the Supplier may also be required to assist with drafting Inquiry reports.
- 1.1.10 Conducting the response to any judicial review- brought against the Inquiry Chair, if required.**

4. KEY MILESTONES AND DELIVERABLES

The following Contract milestones/deliverables shall apply:

6. VOLUMES

6.1 The Inquiry is likely to require advice from the Solicitor to the Inquiry and/or their team on a daily basis. The resource requirement is likely to peak during the periods where the Inquiry is holding public hearings and writing reports.

6.2 As this is a call off Contract volumes of work cannot be guaranteed.

7. CONTINUOUS IMPROVEMENT

7.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

7.2 Changes to the way in which the Services are to be delivered must be brought to the attention of the Inquiry Chair and Secretary and agreed prior to any changes being implemented.

8. SUSTAINABILITY

8.1 The supplier will be expected to use the most efficient and cost-effective methods of travel as and when required. Paper usage should be reduced as far as possible, notwithstanding the fact that some records and evidence may be in hard copy only.

9. QUALITY

9.1 Advice should be provided in the timescales requested by the Inquiry. Advice should account for the specific context of public inquiries and consider the Inquiry's compliance with relevant legislation.

9.2 Advice should be provided by those suitably qualified, holding relevant practising certificates, in line with the technical competency and experience required by the Authority.

9.3 Advice should be accurate, pragmatic and efficiently delivered. The Supplier will strike the appropriate balance between covering issues thoroughly and providing unnecessary detail, to consistently deliver a quality service and value for money to the Authority.

10. STAFF AND CUSTOMER SERVICE

10.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

10.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

10.3 The Supplier shall ensure that staff understand the Thirlwall Inquiry's vision and objectives and will provide excellent customer service to the Thirlwall Inquiry throughout the duration of the Contract.

10.4 The supplier must meet the following experience and requirements:

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

Crown Copyright 2018

- Experience in the conduct of large-scale national inquiries relating to sensitive subject matters involving multiple participants, or cases similar in breadth and scope;
- Experience of dealing with victims and families of victims of unlawful killings, and experience of large-scale national inquiries with significant police interaction, and concurrent criminal investigations or trials.
- Willingness to travel between London and Chester and to spend concentrated periods of time in Chester to support public hearings and to fulfil other duties.

10.5 Ability to provide sufficient resources over a sustained period of time, as the Inquiry is likely to last in the region of 3 years.

11. SERVICE LEVELS AND PERFORMANCE

11.1 The Authority will measure the quality of the Supplier's delivery by:

12.1.1 Quality of Relationships

12.1.2 Timeliness of Work

KPI/SLA	Service Area	KPI/SLA description	Target
13.1.1a	Quality of Relationships	The Authority is to be notified of any issues* with working relationships between Inquiry Secretariat and Supplier teams within 12 working days.	95-98%
13.1.1b	Quality of Relationships	Adjustments to working relationships within the Inquiry Secretariat and Supplier teams following an issue* being notified to be made within 12 working days of such notification	95-98%
*Issues here constitute those that will have a material impact on the delivery of the requirements set out in this Statement of Requirements.			
13.1.2	Timelines of work	Requests from the Inquiry Secretariat labelled 'urgent' must be responded to by the Supplier within 2 working days.	98% of requests responded to within the deadline

12. SECURITY AND CONFIDENTIALITY REQUIREMENTS

- 12.1 The supplier will ensure that all data and information is handled in accordance with the Inquiry's policies and protocols.
- 12.2 Any data breaches will be handled appropriately, including being reported to the Data Protection Officer in a timely fashion.

13. PAYMENT AND INVOICING

- 13.1 Invoices should be issued monthly in arrears by the 15th day of each calendar month.
- 13.2 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
- 13.3 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
- 13.4 Invoices should be submitted to [REDACTED] initially and then be forwarded to accounts payable at DHSC as described in payment method above.

14. CONTRACT MANAGEMENT

- 14.1 Contract Review meetings shall take place on a quarterly basis.
- 14.2 Indicative items for discussion, but not limited to:
 - 16.2.2 Planning for the next quarter
 - 16.2.2 Delivery of previous quarter
 - 16.2.3 Finance and forecasting
 - 16.2.4 KPIs
 - 16.2.5 Risks and Issues
 - 16.2.6 Management Information Reporting
- 16.3 Such meetings are likely to take place online, but where physical attendance is required at Contract Review meetings, this shall be at the Supplier's own expense.

15. LOCATION

- 15.1 The location of the Services will be carried out at the offices of Burges Salmon LLP and Fieldfisher LLP, and the Thirlwall Inquiry, and at hearings in Chester. Some home working will also be possible.

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;

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

Crown Copyright 2018

- (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

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

Crown Copyright 2018

- 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;

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

Crown Copyright 2018

- (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).

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

Crown Copyright 2018

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

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

Crown Copyright 2018

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.

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

Crown Copyright 2018

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.

- 1.1 The contact details of the [REDACTED]
- 1.2 The contact details of the Supplier's [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 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 Parties are Independent Controllers of Personal Data</p> <p>The Supplier is an independent data controller when providing legal services to the Inquiry.</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> ● Business contact details of Supplier Personnel for which the Supplier is the Controller, ● Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller,
Duration of the Processing	The duration of the contract.

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

Crown Copyright 2018

Nature and purposes of the Processing	The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data (whether or not by automated means) etc.
Type of Personal Data	Examples here include names, address, date of birth, telephone number, images, biometric data etc.
Categories of Data Subject	Examples include Core Participants to the Inquiry, witnesses to the Inquiry, Individuals identified in evidence.
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	To be destroyed by the Supplier following the completion of the Inquiry, except where the Supplier is under a professional or legal obligation to retain certain data.

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/Relevant Authority]:

- (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 UKGDPR;
- (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

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

- (a) report to the other Party every 6 months on:

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

Crown Copyright 2018

- (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;

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

Crown Copyright 2018

- (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.

2.2 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

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:

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

Crown Copyright 2018

- (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.

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:

- (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

4.1 The Supplier shall permit:

WORK\49897461\v.1

Framework Ref: RM6179

Project Version: v1.0

Model Version: v3.7

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

Crown Copyright 2018

- (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.
- 4.2 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

5.1 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

- 7.1 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:

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

Crown Copyright 2018

- (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).
- 7.2 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.
- 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"):
- (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.

7.4 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

- 9.1 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.