Crown Commercial Service

Call-Off Order Form for RM6187 Management Consultancy Framework Three (MCF3)

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

Order Form

Call-off reference:	SR857944218
The buyer: "CUSTOMER" or “you”)	HM Revenue & Customs (HMRC) (“Buyer”,
Buyer address:	5th Floor West, Ralli Quays, 3 Stanley Street, Manchester, M60 9LA
The supplier:	Deloitte LLP ("Supplier", “Deloitte” or “we”)
Supplier address:	1 New Street Square, London, EC4A 3HQ
Registration number:	OC 303675
DUNS number:	364807771
Sid4gov id:	364807771

Applicable framework contract

This Order Form is for the provision of the Call-Off Deliverables and dated 01 April 2022
It is issued under the Framework Contract with the reference number RM6187 for the provision of management consultancy services.

Call-off lot: 2. Strategy & Policy

Call-off incorporated terms

The following documents are incorporated into this Call-Off Contract. Where schedules are missing, those schedules are not part of the agreement and cannot be used. 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) RM6187
3. The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data) Appended

Call-Off Schedules

- Call Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 9 (Security) Appended
- Call-Off Schedule 10 (Exit Management)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 18 (Background Checks)
- Call-Off Schedule 20 (Call-Off Specification) Appended
- Call-Off Schedule 23 (HMRC Terms) Appended

4. CCS Core Terms (version 3.0.10 v5)
5. Joint Schedule 5 (Corporate Social Responsibility)
6. Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above**.**

Supplier terms are not 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: 1 April 2022

Call-off expiry date:

Call-off initial period: 12 months

HMRC may at its discretion decide to retain the support of Deloitte to assist with the implementation of the Future Operating Model beyond the Initial Period.

Call-off deliverables:

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

HMRC requires consultancy services to support its Technology Sourcing Programme (TSP). Deloitte will work closely with the Senior Responsible Officer (SRO) and Programme Director to define, orchestrate and integrate delivery across all workstreams, providing advisory input and advice on how to accelerate delivery if required.

Maximum liability

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

The Estimated Year 1 Charges used to calculate liability in the first contract year are: £15,000,000 (excluding VAT)

Call-off charges

The anticipated value of the Contract is £15,000,000 excluding VAT, covering the 12-month Initial Period of the contract and covering:

- Programme Delivery Support: [REDACTED]
- Future Operating Model Detailed Design: [REDACTED]
- Integration “Burst” support : [REDACTED]

The Services will be delivered on a time and materials basis, managed by HMRC in line with approved spending limits. TSP is a fast-paced Programme, and Deloitte will be expected to respond at pace to support Programme priorities as they emerge.

Additional Statements of Work may be agreed between the parties as the work progresses from time to time.

HMRC may at its discretion decide to retain the support of Deloitte to assist with the implementation of the Future Operating Model beyond the Initial Period.

Other Matters:

1) Supplier will be responsible for delivery of activities described in Schedule 20.
2) Activities will be in support of outputs to be delivered by the workstreams, aligned to Programme outcomes.
3) Outputs will be agreed monthly with the relevant Workstream Lead and, where required, the Programme Director.
4) Deloitte will report weekly to the relevant Workstream Lead on the progress of their activities, the status of their outputs and any risks / issues in delivery.
5) Supplier performance in delivery of the activities will be managed via weekly meetings between the Deloitte Engagement Partner (Hywel Madden) and the Programme Director.

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices)

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law
- Benchmarking using Call-Off Schedule 16 (Benchmarking)

Reimbursable expenses

Recoverable as stated in Framework Schedule 3 (Framework Prices) paragraph 4.

Reimbursable Expenses are not permitted within the M25 Greater London area unless expressly permitted by the HMRC Work Manager.

Reimbursable Expenses incurred for activity outside of the M25 Greater London area will be permitted with the prior agreement of the HMRC Work Manager, in accordance with HMRC's T&S Policy.

Payment method

The Supplier shall invoice the Customer monthly in arrears.
HMRC operates with the SAP Ariba Buying and Invoicing platform internally badged as myBUY, therefore the Supplier will be obliged to receive Purchase Orders from and transact invoices back to HMRC over the Ariba network.

Buyer's invoice address

Payments will be directed through the HMRC SAP Ariba Network

Buyer's authorised representative

[REDACTED]
Commercial Deputy Director, Corporate Services Category
[REDACTED]

HMRC, 14 Westfield Avenue, Stratford, London, E20 1HZ

Buyer's security policy

Appended at Call-Off Schedule 9

The Supplier's team must ensure that when they are using equipment provided by the Customer they must comply with the Customer's ICT/Security policies.

When the Supplier's team members are accessing the Customer's systems using the Customer's equipment the ICT/Security policies can be located at the following URL:

https://intranet.prod.dop.corp.hmrc.gov.uk/section/how-do-i/get-help-security/securityinformation-zone

The Supplier must ensure that all team members are made aware of the need to comply with ICT/Security policies and that team members are directed to where the security policies are located.

Supplier's authorised representative

[REDACTED]
Partner, Deloitte LLP
[REDACTED]
1 New Street Square, London, EC4A 3HQ

Supplier's contract manager

[REDACTED]
Director, Deloitte LLP
[REDACTED]
1 New Street Square, London, EC4A 3HQ

Progress report frequency

Progress report to be provided to Programme Director weekly.

Progress meeting frequency

Weekly progress meeting to be held between Supplier Partner and HMRC TSP Programme Director.

Key staff

[REDACTED]

Key subcontractor(s)

Not applicable

Commercially sensitive information

Any information relating to the following provided by the Supplier will be considered to be commercially sensitive/confidential and exempt from disclosure under the Freedom of Information Act 2000 ("FOIA"):

- Personal information (CV's, contact details etc.)
- Pricing, including details of our cost base or insurance arrangements
- Proprietary information
- Approach and/or methodologies

The Government's Transparency Agenda may require the publication of Government contracts. In accordance with guidance issued by GPS and the Code of Practice for FOIA, the Customer will consult the Supplier regarding the redaction (as envisaged in the GPS guidance and Code of Practice) of certain parts of the contract, including those areas identified above.

Service credits

Not applicable

Additional insurances

Not applicable

Guarantee

Not applicable

Buyer's environmental and social value policy

HMRC Sustainable Procurement Strategy available online at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/310632/HMRC_Sustainable_Procurement_Strategy.pdf

HMRC complies with the requirements outlined in the Social Value Model, introduced under PPN 06/20.

Social value commitment

The Supplier agrees, in performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender).

[REDACTED]

Formation of call off contract

By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

For and on behalf of the Supplier:

Signature:

Name:

Role:

Date:

For and on behalf of the Buyer:

Signature:

Name:

Role:

Date:

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

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

"Breach of Security"	1 the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, 2 in either case as more particularly set out in the Security Policy where the Buyer has required

	compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	3 the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

2. Complying with security requirements and updates to them

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

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

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

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

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

3. Security Standards

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

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

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

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

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

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

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

4. Security Management Plan

4.1 Introduction

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

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

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

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

c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government

Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

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

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

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

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

4.3 Development of the Security Management Plan

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

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

Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

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

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

4.4 Amendment of the Security Management Plan

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

a) emerging changes in Good Industry Practice;

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

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

d) any new perceived or changed security threats; and

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

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

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

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

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

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

5. Security breach

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

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

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

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

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

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

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

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

Annex A – Draft Security Management Plan

[REDACTED]

Joint Schedule 11 (Processing Data)

Definitions

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

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

Status of the Controller

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

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

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

Where one Party is Controller and the other Party its Processor

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

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

- The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
  - a systematic description of the envisaged Processing and the purpose of the Processing;
  - an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;
  - an assessment of the risks to the rights and freedoms of Data Subjects; and
  - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

- The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
  - Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
  - ensure that it has in place Protective Measures, including in the case of the 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:
    - nature of the data to be protected;
    - harm that might result from a Personal Data Breach;

- state of technological development; and
- cost of implementing any measures;

- ensure that :
  - the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));
  - it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
    - are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*) of the Core Terms;
    - are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
    - are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
    - have undergone adequate training in the use, care, protection and handling of Personal Data;
- not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
  - the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
  - the Data Subject has enforceable rights and effective legal remedies;
  - the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  - the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

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

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

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

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

- assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

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

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

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

- Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
  - notify the Controller in writing of the intended Subprocessor and Processing;
  - obtain the written consent of the Controller;
  - enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
  - provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

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

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

- The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the 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

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

Independent Controllers of Personal Data

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

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

- Where a Party has provided Personal Data to the other Party in accordance with paragraph 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.

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

- The Parties shall only provide Personal Data to each other:

  - to the extent necessary to perform their respective obligations under the Contract;

  - in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

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

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

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

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

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

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

    - promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

    - provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

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

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

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

- Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*
- Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.
- Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the 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.

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

1.1.1.2 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** [REDACTED]
Duration of the Processing	For the term of the Call Off Contract
Nature and purposes of the Processing	[REDACTED]
Types of Personal Data and Categories of Data Subjects	[REDACTED]

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	[REDACTED]

Call-Off Schedule 20 (Call-Off Specification)

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

[REDACTED]

Call-Off Schedule 23 (HMRC Terms)

1) Definitions

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

"Connected Company"	in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person;
"Control"	the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;
"Prohibited Transaction"	• any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description otherwise payable by the Supplier or a Connected Company on or in connection with the Charges; or 7. which would be payable by any Key Subcontractor and its Connected Companies on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract, other than transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties' business;
"Purchase Order Number"	the Buyer's unique number relating to the supply of the Deliverables;
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably verify the accuracy of any invoice; and
"Tax	where an entity or person under consideration meets all 3

Compliance Failure"	conditions contained in the relevant excerpt from HMRC's "Test for Tax Non-Compliance", as set out in Annex 1 (as amended and updated from time to time), where: • the "Economic Operator" means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Paragraph 5.3; and Schedule 2 any "Essential Subcontractor" means any Key Subcontractor.

- Exclusion of certain Core Terms and terms of Schedules
  - When the Parties have entered into a Call-Off Contract which incorporates the terms of this Call-Off Schedule 23, the following Core Terms are modified in respect of that Call-Off Contract (but are not modified in respect of the Framework Contract):
    - Clauses 31.1, 31.2, 31.3 and 31.4(d) of the Core Terms do not apply to that Call-Off Contract, but for the avoidance of doubt, the remainder of Clause 31.4 of the Core Terms shall continue to apply to the Call-Off Contract; and
    - Clause 7.2 of the Core Terms does not apply to that Call-Off Contract.
  - When the Parties have entered into a Call-Off Contract which incorporates the terms of this Call-Off Schedule 23, the following Joint Schedules are modified in respect of that Call-Off Contract (but are not disapplied in respect of the Framework Contract):
    - The definition of "Occasion of Tax Non-Compliance" contained in Joint Schedule 1 (Definitions) does not apply to that Call-Off Contract; and
    - paragraph 5(d) of Joint Schedule 11 (Processing Data) does not apply to that Call-Off Contract.
- **Charges, Payment and Recovery of Sums Due**
  - The Supplier shall invoice the Buyer as specified in Clause 4 of the Core Terms as modified by any Framework Special Terms or any Call-Off Special Terms.
  - In addition to the provisions of Clause 4 of the Core Terms and any applicable Framework Special Term or Call-Off Special Term, the Supplier shall procure a Purchase Order Number from the Buyer before any Deliverables are supplied. Should the Supplier supply Deliverables without a Purchase Order Number:
    - the Supplier does so at its own risk; and

- the Buyer shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

- The Supplier shall submit each invoice and any Supporting Documentation required in accordance with Clause 4 of the Core Terms and any applicable Framework Special Term or Call-Off Special Term, as directed by the Buyer from time to time, either:

  - via the Buyer 's electronic transaction system as an Electronic Invoice; or

  - to the Programme Director by email in pdf format.

- **Warranties**

  - The Supplier represents and warrants that:

    - in the three years prior to the Effective Date, it has complied with all applicable Law related to Tax in the United Kingdom and in the jurisdiction in which it is established;

    - it has notified the Buyer in writing of any Tax Compliance Failure it is involved in; and

    - no proceedings or other steps have been taken (nor, to the best of the Supplier's knowledge, are threatened) for:

      - the winding up of the Supplier;

      - the Supplier's dissolution; or

      - the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue,

      and the Supplier has notified the Buyer of any profit warnings it has issued in the three years prior to the Effective Date.

  - If the Supplier becomes aware that any of the representations or warranties under Paragraphs 4.1.1, 4.1.2 and/or 4.1.3 have been breached, are untrue or misleading, it shall immediately notify the Buyer in sufficient detail to enable the Buyer to make an accurate assessment of the situation.

  - In the event that the warranty given by the Supplier in Paragraph 4.1.2 is materially untrue, this shall be deemed to be an event to which Clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

- **Promoting Tax Compliance**

- The Supplier shall comply with all Law relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.

- The Supplier shall provide to the Buyer the name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or Subcontractor of the Supplier prior to that person supplying any material Deliverables under the Contract.

- Upon a request by the Buyer, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor of the Supplier engaged in supplying Deliverables under the Contract.

- If, at any point during the Call-Off Contract Period, there is a Tax Compliance Failure, the Supplier shall:

    - notify the Buyer in writing within five (5) Working Days of its occurrence; and

    - promptly provide to the Buyer:

        - details of the steps which the Supplier is taking to resolve the Tax Compliance Failure and to prevent it from recurring, together with any mitigating factors that it considers relevant; and

        - such other information in relation to the Tax Compliance Failure as the Buyer may reasonably require.

- The Supplier shall indemnify the Buyer against any liability for Tax (including any interest, penalties or costs incurred) of the Buyer in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Contract.

- Any amounts due under Paragraph 5.5 shall be paid not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Buyer. Any amounts due under Paragraph 5.5 shall not be subject to clause 11.2 of the Core Terms.

- Upon the Buyer's request, the Supplier shall promptly provide information which demonstrates how the Supplier complies with its Tax obligations.

- If the Supplier:

    - fails to comply with Paragraphs 5.1, 5.4.1 and/or 5.7 this may be a material breach of the Contract;

    - fails to comply with a reasonable request by the Buyer that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Paragraph 5.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in a

Tax Compliance Failure this shall be a material breach of the Contract; and/or

- fails to provide acceptable details of steps being taken and mitigating factors pursuant to Paragraph 5.4.2 this shall be a material breach of the Contract;

and any such material breach shall be deemed to be an event to which clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

- In addition to those circumstances listed in clause 15.2 to 15.4 of the Core Terms, the Buyer may internally share any information, including Confidential Information, which it receives under Paragraphs 5.2 to 5.4 (inclusive) and 5.7.

- **Use of Off-shore Tax Structures**

  - The Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place any Prohibited Transactions, unless the Buyer otherwise agrees to that Prohibited Transaction.

  - The Supplier shall notify the Buyer in writing (with reasonable supporting detail) of any proposal for the Supplier, its Connected Companies, or a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall include reasonable supporting detail and make the notification within a reasonable time before the Prohibited Transaction is due to be put in place.

  - If a Prohibited Transaction is entered into in breach of Paragraph 6.1, or circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Buyer. The Parties shall agree (at no cost to the Buyer) any necessary changes to any such arrangements by the undertakings concerned (and the Supplier shall ensure that the Key Subcontractor shall agree, where applicable). The matter will be resolved using clause 34 of the Core Terms if necessary.

  - Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Paragraphs 6.2 and 6.3 shall be deemed to be an event to which clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

- **Data Protection and off-shoring**

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

- not transfer Personal Data outside of the United Kingdom unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

    - the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

    - the Data Subject has enforceable rights and effective legal remedies;

    - the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

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

- Failure by the Processor to comply with the obligations set out in Paragraph 7.1 shall be deemed to be an event to which clause 10.4.1 of the Core Terms applies and Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

- **Commissioners for Revenue and Customs Act 2005 and related Legislation**

    - The Supplier shall comply with, and shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 ("CRCA") to maintain the confidentiality of Government Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of those obligations may lead to a prosecution under Section 19 of CRCA.

    - The Supplier shall comply with, and shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data comply with the obligations set out in the Official Secrets Acts 1911 to 1989 and the obligations set out in Section 182 of the Finance Act 1989. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of those obligations may lead to prosecution under those Acts.

    - The Supplier shall comply with, and shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data comply with the obligations set out in Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Deliverables. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Buyer) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

- The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Staff who will have access to, or are provided with, Government Data in writing of the obligations upon Supplier Staff set out in Paragraphs 8.1, 8.2 and 8.3. The Supplier shall monitor the compliance by Supplier Staff with such obligations.

- The Supplier shall ensure that all Supplier Staff who will have access to, or are provided with, Government Data sign (or have previously signed) a Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Buyer upon demand.

- In the event that the Supplier or the Supplier Staff fail to comply with this Paragraph 8, the Buyer reserves the right to terminate the Contract as if that failure to comply were an event to which clause 10.4.1 of the Core Terms applies.

Annex 1

Excerpt from HMRC's "Test for Tax Non-Compliance"

Condition one (An in-scope entity or person)

1 There is a person or entity which is either: ("X")

1 The Economic Operator or Essential Subcontractor (EOS)

- Part of the same Group of companies of EOS. An entity will be treated as within the same Group of EOS where that entities' financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts*[1];
- Any director, shareholder or other person (P) which exercises control over EOS. 'Control' means P can secure, through holding of shares or powers under articles of association or other document that EOS's affairs are conducted in accordance with P's wishes.

Condition two (Arrangements involving evasion, abuse or tax avoidance)

2 X has been engaged in one or more of the following:

1. Fraudulent evasion[2];
2. Conduct caught by the General Anti-Abuse Rule[3];
3. Conduct caught by the Halifax Abuse principle[4];
4. Entered into arrangements caught by a DOTAS or VADR scheme[5];

[1] https://www.iasplus.com/en/standards/ifrs/ifrs10

[2] 'Fraudulent evasion' means any 'UK tax evasion offence' or 'UK tax evasion facilitation offence' as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act.

[3] "General Anti-Abuse Rule" means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any future legislation introduced into Parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions

[4] "Halifax Abuse Principle" means the principle explained in the CJEU Case C-255/02 Halifax and others

[5] A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in

5. Conduct caught by a recognised 'anti-avoidance rule'[6] being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. 'Targeted Anti-Avoidance Rules' (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;

6. Entered into an avoidance scheme identified by HMRC's published Spotlights list[7];

7. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))

3 X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:

1. In respect of (a), either X:

   (a) Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure[8]; or,

   (b) Has been charged with an offence of fraudulent evasion.

2. In respect of (b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.

3. In respect of (b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.

secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

[6]The full definition of 'Anti-avoidance rule' can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly.

[7]Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight

[8]The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed.

4. In respect of (f) this condition is satisfied without any further steps being taken.

5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time including any implementing or successor legislation.

Annex 2 Form

CONFIDENTIALITY DECLARATION

CONTRACT REFERENCE: [for Supplier to insert Contract reference number and contract date] ((‘the Agreement’)

DECLARATION:

I solemnly declare that:

1) I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Government Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
- I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Government Data provided to me.

SIGNED:
FULL NAME:
POSITION:
COMPANY:
DATE OF SIGNATURE: