



# COUNCIL OF THE ISLES OF SCILLY

Town Hall, St Mary's, Isles of Scilly, TR21 0LW

☎0300 1234 105

✉enquiries@scilly.gov.uk



**European Union**

European Regional  
Development Fund



Southern Horizons (UK) Ltd  
c/o Blackwell Bate  
122 Fore Street  
Saltash  
Cornwall  
PL12 6JW

Attn: Dr Rebekah Southern

By email to: [rebekah@southernhorizons.co.uk](mailto:rebekah@southernhorizons.co.uk)

Date: 06/04/2022

Your ref: 08098961/GB 136 9958 59

Our ref: PO -P510004130

Dear Sirs,

**Award of contract for the supply of Summative Assessment Project Evaluation Services for Voucher Scheme Extension project**

Following your proposal for the supply of a [**Summative Assessment Project Evaluation Services for Voucher Scheme Extension project**] to the Council of the Isles of Scilly we are pleased to award this contract to you.

This letter (Award Letter) and its [Annex/Annexes] set out the terms of the contract between the Council of the Isles of Scilly as the Customer and [**Southern Horizons (UK) Ltd**] as the Supplier for the provision of the Services. Unless the context otherwise requires, capitalised expressions used in this Award Letter have the same meanings as in the terms and conditions of contract set out in Annex 1 to this Award Letter (the "**Conditions**"). In the event of any conflict between this Award Letter and the Conditions, this Award Letter shall prevail. Please do not attach any Supplier terms and conditions to this Agreement as they will not be accepted by the Customer and may delay the processes.

For the purposes of the Agreement, the Customer and the Supplier agree as follows:

- 1) The Services shall be performed on the Isles of Scilly, generally across the Local Authority Area and the suppliers offices at PEC, Porth Mellon Industrial Estate, St Mary's, IOS
- 2) The charges for the Services shall be as set out in [Annex 3 / the Supplier's quotation dated **[26/03/2022]**].
- 3) The specification of the Services to be supplied is as set out in [Annex 2 / the Supplier's quotation dated **[26/03/2022]**].
- 4) The Term shall commence on **[04/04/2022]** and the Expiry Date shall be **[30/10/2022 unless extended or subject to early termination]**.
- 5) The address for notices of the Parties are:

**Customer**

Council of the Isles of Scilly,  
Town Hall,  
St Mary's,  
Isles of Scilly,  
TR210LW

Attention: Milena Fallows

Email: Milena.Fallows@scilly.gov.uk

**Supplier**

Southern Horizons (UK) Ltd  
c/o Blackwell Bate  
122 Fore Street  
Saltash  
Cornwall  
PL12 6JW

Attention: *Dr Rebekah Southern*

Email: rebekah@southernhorizons.co.uk

- 6) The following persons are Key Personnel for the purposes of the Agreement:

**Name: Milena Fallows**

**Title: Isles of Scilly Voucher Scheme  
Manager, Strategic Development, CIOS**

- 7) For the purposes of the Agreement the [Staff Vetting Procedures/data security requirements/equality and diversity policy and environmental policy are available upon request.
- 8) The Customer may require the Supplier to ensure that any person employed in the provision of the Services has undertaken a Disclosure and Barring Service check. The Supplier shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of the Services, relevant to the work of the Customer, or is of a type otherwise advised by the Customer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Services.

## Payment

All invoices must be sent, quoting a valid purchase order number (PO Number), to: [invoices@scilly.gov.uk](mailto:invoices@scilly.gov.uk) or Council of the Isles of Scilly, Accounts Payable, PO Box 727, Truro TR1 9GP. Within 10 working days of receipt of your countersigned copy of this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.

To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your customer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment. If you have a query regarding an outstanding payment please contact our Accounts Payable section: either by email to [financeprocessing@cornwall.gov.uk](mailto:financeprocessing@cornwall.gov.uk) (for remittance advice: [paymentscontrol@cornwall.gov.uk](mailto:paymentscontrol@cornwall.gov.uk)) or by telephone 01872 323000 between 09:00-17:00 Monday to Friday.

## Liaison

For general liaison your contact will continue to be Milena Fallows or, in their absence, Nicola Stinson.

We thank you for your co-operation to date, and look forward to forging a successful working relationship resulting in a smooth and successful delivery of the Services. Please confirm your acceptance of the award of this contract by signing and returning the enclosed copy of this letter to Milena Fallows at the above address **within [7]** days from the date of this letter. No other form of acknowledgement will be accepted. Please remember to quote the reference number above in any future communications relating to this contract.

Yours faithfully,

Signed for and on behalf of Council of the Isles of Scilly

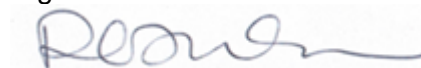
Name: Nicola Stinson

Signature: 

Date: 07/04/22

Name: Rebekah Southern  
Buyer name

Signature:



Date: 7<sup>th</sup> April 2022

We accept the terms set out in this letter and its **Annexes**, including the Conditions.

Signed for and on behalf of **Southern Horizons (UK) Ltd**

Name: Rebekah Southern  
Director

Signature:



Date: 7<sup>th</sup> April 2022

## Annex 1

### Terms and Conditions of Contract for Services

#### 1 Interpretation

1.1 In these terms and conditions:

“Agreement” means this contract;

“Award Letter” means the letter from the Customer to the Supplier printed above these terms and conditions;

“Central Government Body”	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:  (a) Government Department;  (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);  (c) Non-Ministerial Department; or  (d) Executive Agency;
“Charges”	means the charges for the Services as specified in the Award Letter;
“Confidential Information”	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
“Controller”, “Processor”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Data Protection Officer “	take the meaning given in the GDPR
“Customer”	means the person named as Customer in the Award Letter;
“Data Loss Event”	Means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;
“Data Protection Impact Assessment”	means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
“Data Protection Legislation”	means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
“Data Subject Request”	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
“DPA 2018”	means the Data Protection Act 2018;
“Expiry Date”	means the date for expiry of the Agreement as set out in the Award Letter;
“FOIA”	means the Freedom of Information Act 2000;
“GDPR”	Means the General Data Protection Regulation (Regulation (EU) 2016/679)
“Information”	has the meaning given under section 84 of the FOIA;
“Joint Controllers”	where two or more Controllers jointly determine the purposes and means of processing;

“Key Personnel”	means any persons specified as such in the Award Letter or otherwise notified as such by the Customer to the Supplier in writing;
“Law”	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;
“LED”	Law Enforcement Directive (Directive (EU) 2016/680);
“Party”	means a Party to this Agreement;
“Personal Data”	means personal data (as defined in the DPA) which is processed by the Supplier or any Staff on behalf of the Customer pursuant to or in connection with this Agreement;
“Processor Personnel”	means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement
“Protective Measures”	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule C (Baseline Security Requirements).
“Purchase Order Number”	means the Customer’s unique number relating to the supply of the Services;
“Request for Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Services”	means the services to be supplied by the Supplier to the Customer under the Agreement;
“Specification”	means the specification for the Services (including as to quantity, description and quality) as specified in the Award Letter;
“Staff”	means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;
“Staff Vetting Procedures”	means vetting procedures that accord with good industry practice or, where requested by the Customer, the Customer’s procedures for the vetting of personnel as provided to the Supplier from time to time;
“Supplier”	means the person named as Supplier in the Award Letter;
“Sub-processor”	any third Party appointed to process Personal Data on behalf of that Processor related to this Agreement
“Term”	means the period from the start date of the Agreement set out in the Award Letter to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement;

- “VAT” means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
- “Working Day” means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

- 1.2 In these terms and conditions, unless the context otherwise requires:
- 1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;
  - 1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
  - 1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;
  - 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
  - 1.2.5 the word ‘including’ shall be understood as meaning ‘including without limitation’.

## **2 Basis of Agreement**

- 2.1 The Award Letter constitutes an offer by the Customer to purchase the Services subject to and in accordance with the terms and conditions of the Agreement.
- 2.2 The offer comprised in the Award Letter shall be deemed to be accepted by the Supplier on receipt by the Customer of a copy of the Award Letter countersigned by the Supplier within [7] days of the date of the Award Letter.

## **3 Supply of Services**

- 3.1 In consideration of the Customer’s agreement to pay the Charges, the Supplier shall supply the Services to the Customer for the Term subject to and in accordance with the terms and conditions of the Agreement.
- 3.2 In supplying the Services, the Supplier shall:
- 3.2.1 co-operate with the Customer in all matters relating to the Services and comply with all the Customer’s instructions;
  - 3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Supplier’s industry, profession or trade;
  - 3.2.3 use Staff who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number to ensure that the Supplier’s obligations are fulfilled in accordance with the Agreement;
  - 3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;
  - 3.2.5 comply with all applicable laws; and
  - 3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.
- 3.3 The Customer may by written notice to the Supplier at any time request a variation to the scope of the Services. In the event that the Supplier agrees to any variation to the scope of the Services, the Charges shall be subject to fair and reasonable adjustment to be agreed in writing between the Customer and the Supplier.

## **4 Term**

- 4.1 The Agreement shall take effect on the date specified in Award Letter and shall expire on the Expiry Date, unless it is otherwise extended in accordance with clause 4.2 or terminated in

accordance with the terms and conditions of the Agreement.

- 4.2 The Customer may extend the Agreement for a period of up to 6 months by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The terms and conditions of the Agreement shall apply throughout any such extended period.

## **5 Charges, Payment and Recovery of Sums Due**

- 5.1 The Charges for the Services shall be as set out in the Award Letter and shall be the full and exclusive remuneration of the Supplier in respect of the supply of the Services. Unless otherwise agreed in writing by the Customer, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.
- 5.2 The Supplier shall invoice the Customer as specified in the Agreement. Each invoice shall include such supporting information required by the Customer to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.
- 5.3 In consideration of the supply of the Services by the Supplier, the Customer shall pay the Supplier the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number. The Customer may, without prejudice to any other rights and remedies under the Agreement, withhold or reduce payments in the event of unsatisfactory performance.
- 5.4 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Customer shall, following the receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.
- 5.5 If there is a dispute between the Parties as to the amount invoiced, the Customer shall pay the undisputed amount. The Supplier shall not suspend the supply of the Services unless the Supplier is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with clause 15.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 18.
- 5.6 If a payment of an undisputed amount is not made by the Customer by the due date, then the Customer shall pay the Supplier interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.
- 5.7 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Customer in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Customer from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Customer. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Customer in order to justify withholding payment of any such amount in whole or in part.
- 5.8 Where the Supplier submits an invoice to the Authority in accordance with paragraph 5.2, the Authority will consider and verify that invoice in a timely fashion.
- 5.9 The Authority shall pay the Supplier any sums due under such an invoice no later than a period of 30 days from the date on which the Authority has determined that the invoice is valid and undisputed.
- 5.10 Where the Authority fails to comply with paragraph 5.9 and there is an undue delay in considering and verifying the invoice, the invoice shall be regarded as valid and undisputed for the purposes of paragraph 5.9 after a reasonable time has passed.
- 5.11 Where the Supplier enters into a Sub-Contract, the Supplier shall include in that Sub-Contract:

- 5.11.1 Provisions having the same effect as clauses 5.8- 5.10 of this Agreement; and
- 5.11.2 A provision requiring the counterparty to that Sub-Contract to include in any Sub-Contract which it awards provisions having the same effect as clauses 5.8 – 5.11 of this Agreement.
- 5.11.3 In clause 5, “Sub-Contract” means a contract between two or more suppliers, at any stage of remoteness from the Authority in a subcontracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Agreement.

## **6 Premises and equipment**

- 6.1 If necessary, the Customer shall provide the Supplier with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Customer’s premises by the Supplier or the Staff shall be at the Supplier’s risk.
- 6.2 If the Supplier supplies all or any of the Services at or from the Customer’s premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Supplier shall vacate the Customer’s premises, remove the Supplier’s plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Customer’s premises in a clean, safe and tidy condition. The Supplier shall be solely responsible for making good any damage to the Customer’s premises or any objects contained on the Customer’s premises which is caused by the Supplier or any Staff, other than fair wear and tear.
- 6.3 If the Supplier supplies all or any of the Services at or from its premises or the premises of a third party, the Customer may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.
- 6.4 The Customer shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Customer’s premises the Supplier shall, and shall procure that all Staff shall, comply with all the Customer’s security requirements.
- 6.5 Where all or any of the Services are supplied from the Supplier’s premises, the Supplier shall, at its own cost, comply with all security requirements specified by the Customer in writing.
- 6.6 Without prejudice to clause 3.2.6, any equipment provided by the Customer for the purposes of the Agreement shall remain the property of the Customer and shall be used by the Supplier and the Staff only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Customer on expiry or termination of the Agreement.
- 6.7 The Supplier shall reimburse the Customer for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Supplier or any Staff. Equipment supplied by the Customer shall be deemed to be in a good condition when received by the Supplier or relevant Staff unless the Customer is notified otherwise in writing within 5 Working Days.

## **7 Staff and Key Personnel**

- 7.1 If the Customer reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Supplier:
  - 7.1.1 refuse admission to the relevant person(s) to the Customer’s premises;
  - 7.1.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s); and/or



- 7.1.3 require that the Supplier replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Customer to the person removed is surrendered,

and the Supplier shall comply with any such notice.

7.2 The Supplier shall:

- 7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures;  
7.2.2 if requested, provide the Customer with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Customer's premises in connection with the Agreement; and  
7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Customer.

7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Customer, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.

7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Customer (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

## **8 Assignment and sub-contracting**

- 8.1 The Supplier shall not without the written consent of the Customer assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement. The Customer may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Supplier shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.
- 8.2 Where the Supplier enters into a sub-contract for the purpose of performing its obligations under the Agreement, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Supplier to the sub-contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.
- 8.3 Where the Customer has consented to the placing of sub-contracts, the Supplier shall, at the request of the Customer, send copies of each sub-contract, to the Customer as soon as is reasonably practicable.
- 8.4 The Customer may assign, novate, or otherwise dispose of its rights and obligations under the Agreement without the consent of the Supplier provided that such assignment, novation or disposal shall not increase the burden of the Supplier's obligations under the Agreement.

## **9 Intellectual Property Rights**

- 9.1 All intellectual property rights in any materials provided by the Customer to the Supplier for the purposes of this Agreement shall remain the property of the Customer but the Customer hereby grants the Supplier a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Supplier to perform its obligations under the Agreement.
- 9.2 All intellectual property rights in any materials created or developed by the Supplier pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Supplier. If, and to the extent, that any intellectual property rights in such materials vest in the Customer by operation of law, the Customer hereby assigns to the Supplier by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).

9.3 The Supplier hereby grants the Customer:

9.3.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Agreement and any intellectual property rights arising as a result of the provision of the Services; and

9.3.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

(a) any intellectual property rights vested in or licensed to the Supplier on the date of the Agreement; and

(b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which the Customer reasonably requires in order to exercise its rights and take the benefit of the Agreement including the Services provided.

9.4 The Supplier shall indemnify, and keep indemnified, the Customer in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by the Customer as a result of or in connection with any claim made against the Customer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Supplier or any Staff.

## 10 Governance and Records

10.1 The Supplier shall:

10.1.1 attend progress meetings with the Customer at the frequency and times specified by the Customer and shall ensure that its representatives are suitably qualified to attend such meetings; and

10.1.2 submit progress reports to the Customer at the times and in the format specified by the Customer.

10.2 The Supplier shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Customer. The Supplier shall on request afford the Customer or the Customer's representatives such access to those records as may be reasonably requested by the Customer in connection with the Agreement.

## 11 Confidentiality, Transparency and Publicity

11.1 Subject to clause 11.2, each Party shall:

11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:

11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

11.2.2 to its auditors or for the purposes of regulatory requirements;

- 11.2.3 on a confidential basis, to its professional advisers;
- 11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;
- 11.2.5 where the receiving Party is the Supplier, to the Staff on a need to know basis to enable performance of the Supplier's obligations under the Agreement provided that the Supplier shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Supplier's confidentiality obligations under the Agreement; and
- 11.2.6 where the receiving Party is the Customer:
  - (a) on a confidential basis to the employees, agents, consultants and contractors of the Customer;
  - (b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Customer transfers or proposes to transfer all or any part of its business;
  - (c) to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or
  - (d) in accordance with clause 12.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Customer under this clause 11.

- 11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Supplier hereby gives its consent for the Customer to publish this Agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Customer may consult with the Supplier to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.
- 11.4 The Supplier shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Customer.

## **12 Freedom of Information**

- 12.1 The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:
  - 12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;
  - 12.1.2 transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 Working Days of receipt;
  - 12.1.3 provide the Customer with a copy of all Information belonging to the Customer requested in the Request for Information which is in its possession or control in the form that the Customer requires within 5 Working Days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and

12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Customer.

12.2 The Supplier acknowledges that the Customer may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Supplier or the Services (including commercially sensitive information) without consulting or obtaining consent from the Supplier. In these circumstances the Customer shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Supplier advance notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

12.3 Notwithstanding any other provision in the Agreement, the Customer shall be responsible for determining in its absolute discretion whether any Information relating to the Supplier or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

### **13 Data Protection**

13.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule A. The only processing that the Processor is authorised to do is listed in Schedule A by the Controller and may not be determined by the Processor.

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

13.3 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:

13.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;

13.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

13.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

13.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

13.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

13.4.1 process that Personal Data only in accordance with Schedule A, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

13.4.2 ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, 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:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

13.4.3 ensure that :

(a) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Schedule A);

- (b) 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:
    - I) are aware of and comply with the Processor's duties under this clause;
    - II) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
    - III) 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 this Agreement; and
    - IV) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- 13.4.4 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:
  - (a) 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;
  - (b) the Data Subject has enforceable rights and effective legal remedies;
  - (c) 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
  - (d) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
- 13.4.5 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.
- 13.5 Subject to clause 13.6, the Processor shall notify the Controller immediately if it:
  - 13.5.1 receives a Data Subject Request (or purported Data Subject Request);
  - 13.5.2 receives a request to rectify, block or erase any Personal Data;
  - 13.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
  - 13.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
  - 13.5.5 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
  - 13.5.6 becomes aware of a Data Loss Event.
- 13.6 The Processor's obligation to notify under clause 13.5 shall include the provision of further information to the Controller in phases, as details become available.
- 13.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 13.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- 13.7.1 the Controller with full details and copies of the complaint, communication or request;
  - 13.7.2 such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
  - 13.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
  - 13.7.4 assistance as requested by the Controller following any Data Loss Event;
  - 13.7.5 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.
- 13.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- 13.8.1 the Controller determines that the processing is not occasional;
  - 13.8.2 the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
  - 13.8.3 the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 13.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 13.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
- 13.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:
- 13.11.1 notify the Controller in writing of the intended Sub-processor and processing;
  - 13.11.2 obtain the written consent of the Controller;
  - 13.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 13 such that they apply to the Sub-processor; and
  - 13.11.4 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
- 13.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.
- 13.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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 this Agreement).
- 13.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.
- 13.15 Where the Parties include two or more Joint Controllers as identified in Schedule A in accordance with GDPR Article 26, those Parties shall enter into a Joint Controller Agreement based on the terms outlined in Schedule B in replacement of Clauses 13.1-13.14 for the Personal Data under Joint Control Liability.

## 14 Force Majeure

Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Supplier. Each Party shall promptly notify the other Party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If such circumstances continue for a continuous period of more than two months, either Party may terminate the Agreement by written notice to the other Party.

## 15 Termination

- 15.1 The Customer may terminate the Agreement at any time by notice in writing to the Supplier to take effect on any date falling at least 1 month (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.
- 15.2 Without prejudice to any other right or remedy it might have, the Customer may terminate the Agreement by written notice to the Supplier with immediate effect if the Supplier:
  - 15.2.1 (without prejudice to clause 15.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;
  - 15.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;
  - 15.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;
  - 15.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;
  - 15.2.5 breaches any of the provisions of clauses 7.2, 11, 12, **Error! Reference source not found.** and 16; or
  - 15.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Supplier (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Supplier's assets or business, or if the Supplier makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 15.2.6) in consequence of debt in any jurisdiction.
- 15.3 The Supplier shall notify the Customer as soon as practicable of any change of control as referred to in clause 15.2.4 or any potential such change of control.
- 15.4 The Supplier may terminate the Agreement by written notice to the Customer if the Customer has not paid any undisputed amounts within 90 days of them falling due.
- 15.5 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, **Error! Reference source not found.**, 13.1, 15.6, 16.4, 17.3, 18 and 19.7 or any other provision of the Agreement that either expressly or by implication has effect after termination.
- 15.6 Upon termination or expiry of the Agreement, the Supplier shall:
  - 15.6.1 give all reasonable assistance to the Customer and any incoming supplier of the Services; and
  - 15.6.2 return all requested documents, information and data to the Customer as soon as reasonably practicable.

## 16 Compliance

- 16.1 The Supplier shall promptly notify the Customer of any health and safety hazards which may

arise in connection with the performance of its obligations under the Agreement. The Customer shall promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer's premises and which may affect the Supplier in the performance of its obligations under the Agreement.

**16.2 The Supplier shall:**

- 16.2.1 comply with all the Customer's health and safety measures while on the Customer's premises; and
- 16.2.2 notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Agreement on the Customer's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

**16.3 The Supplier shall:**

- 16.3.1 perform its obligations under the Agreement in accordance with all applicable equality Law and the Customer's equality and diversity policy as provided to the Supplier from time to time; and
- 16.3.2 take all reasonable steps to secure the observance of clause 16.3.1 by all Staff.

**16.4 The Supplier shall supply the Services in accordance with the Customer's environmental policy as provided to the Supplier from time to time.**

**16.5 The Supplier shall comply with, and shall ensure that its Staff shall comply with, the provisions of:**

- 16.5.1 the Official Secrets Acts 1911 to 1989; and
- 16.5.2 section 182 of the Finance Act 1989.

**17 Prevention of Fraud and Corruption**

**17.1 The Supplier shall not offer, give, or agree to give anything, to any person an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Agreement or for showing or refraining from showing favour or disfavour to any person in relation to the Agreement.**

**17.2 The Supplier shall take all reasonable steps, in accordance with good industry practice, to prevent fraud by the Staff and the Supplier (including its shareholders, members and directors) in connection with the Agreement and shall notify the Customer immediately if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.**

**17.3 If the Supplier or the Staff engages in conduct prohibited by clause 17.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Customer) the Customer may:**

- 17.3.1 terminate the Agreement and recover from the Supplier the amount of any loss suffered by the Customer resulting from the termination, including the cost reasonably incurred by the Customer of making other arrangements for the supply of the Services and any additional expenditure incurred by the Customer throughout the remainder of the Agreement; or
- 17.3.2 recover in full from the Supplier any other loss sustained by the Customer in consequence of any breach of this clause.

**18 Dispute Resolution**

**18.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.**

**18.2 If the dispute cannot be resolved by the Parties within one month of being escalated as**



referred to in clause 18.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the “**Mediator**”) chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.

- 18.3 If the Parties fail to appoint a Mediator within one month, or fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, either Party may exercise any remedy it has under applicable law.

## **19 General**

- 19.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.
- 19.2 A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties.
- 19.3 The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.
- 19.4 The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.
- 19.5 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.
- 19.6 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party’s behalf.
- 19.7 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
- 19.8 If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.

## **20 Notices**

- 20.1 Any notice to be given under the Agreement shall be in writing and may be served by personal delivery, first class recorded or, subject to clause 20.3, e-mail to the address of the relevant Party set out in the Award Letter, or such other address as that Party may from time to time notify to the other Party in accordance with this clause:
- 20.2 Notices served as above shall be deemed served on the Working Day of delivery provided delivery is before 5.00pm on a Working Day. Otherwise delivery shall be deemed to occur on the next Working Day. An email shall be deemed delivered when sent unless an error message is received.

- 20.3 Notices under clauses 14 (Force Majeure) and 15 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 20.1.

## **21 Governing Law and Jurisdiction**

- 21.1 The validity, construction and performance of the Agreement, and all contractual and non contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

## **22 Safeguarding**

- 22.1 The Service Provider shall develop and maintain awareness and understanding of safeguarding issues with vulnerable adults, children and young people.
- 22.2 The Service Provider shall ensure that all allegations, suspicions and incidents of abuse, harm or risk of harm to children and/or vulnerable adults or where there is concern about the behaviour of an individual are reported immediately to the Council's Representative and the Adult Social Care Team in respect of a vulnerable adult or the Children's Social Care Team in respect of a child. The Service Provider's safeguarding policies and procedures should include active encouragement to staff in whistle blowing if aware of suspected abuse.
- 22.3 The Service Provider shall ensure that children and/or vulnerable adults are safeguarded from any form of exploitation including physical, financial, psychological and sexual abuse, neglect, discriminatory abuse or self harm or inhumane or degrading treatment through deliberate intent, negligent acts or omissions.
- 22.4 The Service provider shall comply with all statutory obligations and Council and Government policies (including but not limited to the Council's Safeguarding Policy, Safeguarding Guidance for Providers and the South West Safeguarding Procedures) in respect of safeguarding as applicable and amended from time to time.
- 22.5 The Service Provider shall immediately notify the Council of any information that it reasonably requests to enable it to be satisfied that the obligations of this clause 23 have been met.
- 22.6 The Service Provider must comply with any instruction given by the Council in respect of this clause 23
- 22.7 The Parties acknowledge that the Service Provider is a Regulated Activity Provider with ultimate responsibility for the management and control of the Regulated Activity provided under this Contract and for the purposes of the Safeguarding Vulnerable Groups Act 2006.
- 22.8 The Service Provider shall:
- 22.8.1 ensure that all individuals engaged in Regulated Activity are subject to a valid enhanced disclosure check for regulated activity undertaken through the Disclosure and Barring Service; and
  - 22.8.2 monitor the level and validity of the checks under this clause 23 for each member of staff;
  - 22.8.3 not employ or use the services of any person who is barred from, or whose previous conduct or records indicate that he or she would not be suitable to carry out Regulated Activity or who may otherwise present a risk to Service Users.

- 22.9 The Service Provider warrants that at all times for the purposes of this Agreement it has no reason to believe that any person who is or will be employed or engaged by the Service Provider in the provision of the Services is barred from activity in accordance with the provisions of the Safeguarding Vulnerable Groups Act 2006 and any regulations made thereunder, as amended from time to time.
- 22.10 The Service Provider shall refer information about any person carrying out the Services to the DBS where it removes permission for such person to carry out the Services (or would have, if such person had not otherwise ceased to carry out the Services) because, in its opinion, such person has harmed or poses a risk of harm to the Service Users, children or vulnerable adults.
- 22.11 The Service Provider shall ensure that all personnel engaged in the delivery of the Services regularly receive appropriate safeguarding training in relation to children and/or vulnerable adults in accordance with the Specification or as agreed by the Parties
- 22.12 The Service Provider shall appoint an individual of sufficient seniority for the safeguarding of children and/or vulnerable adults. This individual shall be responsible for the implementation and monitoring of the Service Provider's safeguarding policies and procedures in accordance with the terms of this Agreement.
- 22.13 The Service Provider shall ensure that it operates a recruitment and selection procedure which aligns with the Council's safer recruitment and disciplinary standards and which meets the requirements of legislation, equal opportunities and anti-discriminatory practice and ensures the protection of children and vulnerable adults.

## **23 Whistleblowing**

- 23.1 The Service Provider shall:
- 23.1.1 have in place a process whereby its employees may report in confidence any alleged malpractice on the part of the Service Provider as regards any part of the provision of the Services;
- 23.1.2 not take any action against any employee pursuant to its contractual rights in respect of that employee where such employee has in accordance with the process provided pursuant to clause 24.1.1 and in good faith reported alleged malpractice on the part of the Service Provider

## Schedule A Processing, Personal Data and Data Subjects

This Schedule 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 Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: **Simon Mansell**  
Contact details [Simion.Mansell@cornwall.gov.uk](mailto:Simion.Mansell@cornwall.gov.uk)
2. The contact details of the Processor's Data Protection Officer are: **[Insert]** Contact details]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	<p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 13.1.</p> <p><b>[Guidance:</b> You may need to vary this section where (in the rare case) the Customer and Contractor have a different relationship. For example where the Parties are Joint Controller of some Personal Data:</p> <p><i>"Notwithstanding Clause 13.1 the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <p><b>[Insert]</b> the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]</p> <p><i>In respect of Personal Data under Joint Control, Clause 13.1-13.15 will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule Y instead."</i></p>
Subject matter of the processing	<p><i>[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.</i></p> <p><i>Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public. ]</i></p>
Duration of the processing	<p><i>[Clearly set out the duration of the processing including dates]</i></p>
Nature and purposes of the processing	<p><i>[Please be as specific as possible, but make sure that you cover all intended purposes.</i></p> <p><i>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by</i></p>

	<p><i>transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i></p>
Type of Personal Data being Processed	<i>[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]</i>
Categories of Data Subject	<i>[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]</i>
<p>Plan for return and destruction of the data once the processing is complete</p> <p>UNLESS requirement under union or member state law to preserve that type of data</p>	<i>[Describe how long the data will be retained for, how it be returned or destroyed]</i>

## Schedule B: Joint Controller Agreement

**[Guidance:** insert only where Joint Controller applies in Schedule A]

In this Annex the Parties must outline each party's responsibilities for:

- providing information to data subjects under [Article 13 and 14](#) of the GDPR.
- responding to data subject requests under [Articles 15-22](#) of the GDPR
- notifying the Information Commissioner (and data subjects) where necessary about data breaches
- maintaining records of processing under [Article 30](#) of the GDPR
- carrying out any required Data Protection Impact Assessment
- The agreement must include a statement as to who is the point of contact for data subjects.

The essence of this relationship shall be published.

You may wish to incorporate some clauses equivalent to those specified in Clause 13.2-13.14.

You may also wish to include an additional clause apportioning liability between the parties arising out of data protection; of data that is jointly controlled.

Where there is a Joint Control relationship, but no controller to processor relationship under the contract, this completed Schedule B should be used instead of Clause 13.1-13.15.

## Schedule C: Baseline Security Requirements

### 1 Definitions

In this Schedule, the following definitions shall apply:

"Information Management System"	means the Core Information Management System and the Wider Information Management System;
"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Services, the Authority Premises, the Sites, the Supplier System, the Authority System and/or any information or data (including the Confidential Information and the Authority Data) used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data (including the Confidential Information and the Authority Data), including copies of such information or data, used by the Authority, the Supplier or any Sub-contractor in connection with this Agreement;
"Core Information Management System"	those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data, together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources;
Personal Data	has the meaning given in the Data Protection Legislation;
Personal Data Breach	has the meaning given in the Data Protection Legislation;
"Process Authority Data"	any operation which is performed on Authority Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Authority Data;
"Wider Information Management System"	" those information assets, ICT systems and/or Sites which will be used by the Supplier and/or its Sub-contractors to Process Authority Data which have not been determined by the Authority to form part of the Core Information Management System together with the associated information management system (including organisational structure, controls, policies, practices, procedures, processes and resources.

## **2 Security Classification of Information**

If the provision of the Services requires the Supplier to Process Authority Data which is classified as:

- 2.1 OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards; and/or
- 2.2 SECRET or TOP SECRET, the Supplier shall only do so where it has notified the Authority prior to receipt of such Authority Data and the Supplier shall implement additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

## **3 End User Devices**

- 3.1 The Supplier shall ensure that any Authority Data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.
- 3.2 The Supplier shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

## **4 Networking**

The Supplier shall ensure that any Authority Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

## **5 Personnel Security**

- 5.1 All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.
- 5.2 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those



individuals with privileged access to IT systems which Process Authority Data or data which is classified as OFFICIAL-SENSITIVE.

- 5.3 The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
- 5.4 The Supplier shall ensure that Supplier Personnel are only granted such access to Authority Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
- 5.5 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.

## **6 Identity, Authentication and Access Control**

- 6.1 The Supplier shall ensure that Supplier Personnel who no longer require access to the Authority Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within 1 Working Day.
  - 6.1.1 all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
  - 6.1.2 all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
- 6.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.
- 6.3 The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Authority on request.

## **7 Audit and Protective Monitoring**

- 7.1 The Supplier shall collect audit records which relate to security events in [/ Core] Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting

out details of access by users of the [Core Information Management System], to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

7.2 The Supplier and the Authority shall work together to establish any additional audit and monitoring requirements for the Core Information Management System.

7.3 The retention periods for audit records and event logs must be agreed with the Authority and documented.

## **8 Secure Architecture**

8.1 The Supplier shall design the Core Information Management System in accordance with:

8.1.1 the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principlesdigital-services-main>;

8.1.2 the NCSC "Bulk Data Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main>; and

8.1.3 the NSCS "Cloud Security Principles", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles> and which are summarised below:

- (a) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
- (b) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
- (c) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
- (d) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
- (e) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
- (f) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;
- (g) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

- (h) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;
- (i) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;
- (j) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
- (k) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
- (l) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
- (m) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Subcontractors;
- (n) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

## Annex 2

### Charges

As per supplier quotation on 26/03/2022 & pricing spreadsheet submitted

#### 5. Pricing

The total cost for this this evaluation, based on our proposed approached, will be **£20,225 + VAT**. This is based on a total of 46 days of consultancy time plus £750 to cover expenses for a single three day trip to the Islands for two consultants. No third-party costs are included. Please see the attached spread-sheet for a breakdown of fees which represent excellent value for money given the seniority and track-record of the team.

	RS	EB	LB	Totals
Inception and Project Management including updates and meetings	1.5	1		2.5
Development of evaluative framework	2	1		3
Design of data capture tools	2	0.5	1	3.5
Desk based review of key documentation	2	2		4
Stakeholder interviews (telephone)	0	1.5		1.5
Beneficiary interviews (telephone)	1	1	7	9
Three day site visit to include interviews, workshops, case studies and progress meeting include travel	4	4		8
Analysis	2	4	1	7
Reporting	4	3	0.5	7.5
<b>TOTAL DAYS</b>	<b>18.5</b>	<b>18</b>	<b>9.5</b>	<b>46</b>
DAY RATE	£450	£450	£400	
<b>TOTAL FEE FOR CONSULTANCY DAYS</b>	<b>£8,325</b>	<b>£8,100</b>	<b>£3,800</b>	<b>£20,225</b>
Travel & susistence				£750
<b>SUB-TOTAL</b>				<b>£20,975</b>
<a href="#">VAT@ 20%</a>				£4,195
<b>GRAND TOTAL</b>				<b>£25,170</b>

**Annex 3**  
**Specification and Timeframes**  
**As per supplier quotation on 26/03/2022**

- ESIF GN-1-033 - ERDF Summative Assessment Guidance -  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/896857/ESIF-GN-1-033\\_ERDF\\_Summative\\_Assessment\\_Guidance\\_v4.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896857/ESIF-GN-1-033_ERDF_Summative_Assessment_Guidance_v4.pdf)
- ESIF GN 1-034 - ERDF Summative Assessment Guidance –
- [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/915448/ESIF-GN-1-034\\_ERDF\\_Summative\\_Assessment\\_Guidance\\_Appendices\\_v4\\_updated.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915448/ESIF-GN-1-034_ERDF_Summative_Assessment_Guidance_Appendices_v4_updated.pdf)
- *ESIF Form 1-014 – Summative Assessment Report Summary – attached Appendix 1*
- *ESIF- Form 1-012 ERDF Summative Assessment Plan Form 1- attached Appendix 1- please note that Voucher scheme has previously submitted SA plan, which can be amended in Finalisation of methodology phase.*
- ***Updated versions will be made available as soon as possible***

The supplier will be expected to undertake a summative assessment and provide a full report together with a final summary in line with the requirements of this quotation document and above ERDF guidance.

**Supplier's proposed and included in quotation price activities & timeframes as per supplier quotation on 26/03/2022**

<b>Activity</b>	<b>Dates</b>	<b>Lead</b>	<b>Client and stakeholder input</b>
<b>Project Inception (remote meeting)</b>	w/b 4 <sup>th</sup> Apr	Rebekah	Client to host online meeting and provide us with key materials etc. Also, agreement on legal basis for accessing data
<b>Development of evaluation framework</b>	11 <sup>th</sup> – 29 <sup>th</sup> Apr	Rebekah	N/A
<b>Framework discussed, amended where required and signed off (remotely)</b>	By 3 <sup>rd</sup> May	Rebekah	Client to host online meeting and ultimately sign-off the Framework
<b>Drafting of topic guides for stakeholder, delivery team and beneficiary interviews and amendments as required</b>	3 <sup>rd</sup> – 12 <sup>th</sup> May	Rebekah and Lorna	Client to review and sign-off questions (via email unless remote meeting is required)
<b>Topic guides discussed, amended where required and signed off (remotely)</b>	By 16 <sup>th</sup> May	Rebekah and Lorna	Client to review and sign-off questions (via email unless or remote online meeting if required)
<b>Undertake beneficiary interviews</b>	May – mid Aug	Lorna	Legal basis to be determined at project inception
<b>Undertake individual external stakeholder interviews</b>	Jun – mid Aug	Emma	Client to contact stakeholders on our behalf to secure permission for evaluation team to contact them. Selection of key stakeholders (to be agreed) will then be interviewed remotely by the team
<b>Three-day visit to include: Progress meeting Workshops/interviews with delivery team and key stakeholders Case study development</b>	Jul (date TBC)	Rebekah	Client to host progress meeting and help to organise the workshops/interviews which will also involve other delivery team members and wider stakeholders
<b>Desk based review of key documentation</b>	Aug	Rebekah	N/A
<b>Desk based review of wider policy and economic context</b>	Aug	Emma	N/A
<b>Desk based review of monitoring data</b>	Aug	Emma	Client to be available to deal with queries (assuming Q2 2022 cut off)
<b>Analysis of all data including FM and impact</b>	Aug	Emma	N/A
<b>Report writing</b>	Aug – mid Sept	Rebekah	N/A
<b>Draft report produced</b>	By 15 <sup>th</sup> Sept	Rebekah	N/A
<b>Meeting to discuss report</b>	w/b 26 <sup>th</sup> Sept	Rebekah	Client to review report and host remote meeting to discuss