

**CABINET OFFICE**

**- and -**

**IMPROVEMENT AND DEVELOPMENT AGENCY (IDeA), trading arm of the Local Government Association (LGA)**

**ATTACHMENT 5**

**relating to**

**PROVISION OF OGP OPE PROGRAMME**

**CCCC22A09**

**CONTENTS**

[**ANNEX 1 – TERMS AND CONDITIONS** 3](#_heading=h.30j0zll)

[1](#_heading=h.1fob9te) Interpretation 3

[2](#_heading=h.3znysh7) Basis of Agreement 4

[3](#_heading=h.2et92p0) Supply of Services 5

[4](#_heading=h.1t3h5sf) Term 5

[5](#_heading=h.2s8eyo1) Charges, Payment and Recovery of Sums Due 5

[6](#_heading=h.17dp8vu) Premises and equipment 6

[7](#_heading=h.1ksv4uv) Staff and Key Personnel 7

[8](#_heading=h.z337ya) Assignment and sub-contracting 8

[9](#_heading=h.3j2qqm3) Intellectual Property Rights 8

[10](#_heading=h.2xcytpi) Governance and Records 9

[11](#_heading=h.2bn6wsx) Confidentiality, Transparency and Publicity 9

[12](#_heading=h.147n2zr) Freedom of Information 10

[13](#_heading=h.3o7alnk) Protection of Personal Data and Security of Data 11

[14](#_heading=h.32hioqz) Liability 11

[15](#_heading=h.3fwokq0) Force Majeure 12

[16](#_heading=h.1v1yuxt) Termination 12

[17](#_heading=h.1mrcu09) Compliance 13

[18](#_heading=h.3l18frh) Prevention of Fraud and Corruption 14

[19](#_heading=h.3vac5uf) Dispute Resolution 14

[20](#_heading=h.pkwqa1) General 14

[21](#_heading=h.1opuj5n) Notices 15

[22](#_heading=h.3mzq4wv) Governing Law and Jurisdiction 15

[**ANNEX 2 – PRICE SCHEDULE** 16](#_heading=h.2250f4o)

[**ANNEX 3 – STATEMENT OF REQUIREMENTs** 17](#_heading=h.haapch)

[**ANNEX 4 – SUPPLIER’S RESPONSE** 18](#_heading=h.1yyy98l)

[**ANNEX 5 – CLARIFICATIONS** 19](#_heading=h.2y3w247)

[**ANNEX 6 – ADDITIONAL TERMS & CONDITIONS** 20](#_heading=h.1d96cc0)

[**ANNEX 7 – CHANGE CONTROL FORMS** 21](#_heading=h.2hio093)

**ANNEX 1 – TERMS AND CONDITIONS**

1. **Interpretation**
   1. In these terms and conditions:

|  |  |
| --- | --- |
| “Agreement” | means the contract between (i) the Customer acting as part of the Crown and (ii) the Supplier constituted by the Supplier’s countersignature of the Award Letter and includes the Award Letter; |
| “Award Letter” | means the letter (including the Annexes thereto) from the Customer to the Supplier via the e-Sourcing Suite at the point of award; |
| “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:   1. Government Department; 2. Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); 3. Non-Ministerial Department; or 4. 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; |
| “Customer” | means the Contracting Authority/Customer named in the Award Letter; |
| “DPA” | 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; |
| “Information” | has the meaning given under section 84 of the FOIA; |
| “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; |
| “Party” | means the Supplier or the Customer (as appropriate) and “Parties” shall mean both of them; |
| “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; |
| “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; |
| “Start Date” | means the commencement date of the Agreement as set out 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; |
| “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. In these terms and conditions, unless the context otherwise requires:
     1. references to numbered clauses are references to the relevant clause in these terms and conditions;
     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;
     3. the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;
     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
     5. the word ‘including’ shall be understood as meaning ‘including without limitation’.

1. **Basis of Agreement**
   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. The offer comprised in the Award Letter shall be deemed to be accepted by the Supplier on receipt by the Customer, within 7 days of the date of the award letter, of a copy of the Award Letter countersigned by the Supplier.
2. **Supply of Services**
   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.
   2. In supplying the Services, the Supplier shall:
      1. co-operate with the Customer in all matters relating to the Services and comply with all the Customer’s instructions;
      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. 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;
      4. ensure that the Services shall conform with all descriptions, requirements, service levels and specifications set out in the Specification;
      5. comply with all applicable laws; and
      6. provide all equipment, tools and vehicles and other items as are required to provide the Services.
   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.
3. **Term**
   1. The Agreement shall take effect on the Start Date 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.
   2. The Customer may extend the Agreement for a period of up to 2 periods of 1 year 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.
4. **Charges, Payment and Recovery of Sums Due**
   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.
   2. 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.
   3. 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.
   4. 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 verifying that the invoice is valid and undisputed and 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. If the Customer fails to consider and verify an invoice in a timely fashion the invoice shall be regarded as valid and undisputed for the purpose of paragraph 5.4 after a reasonable time has passed.
   6. 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 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.
   7. 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.
   8. Where the Supplier enters into a sub-contract, the Supplier shall include in that sub-contract:
      1. provisions having the same effects as clauses 5.3 to 5.7 of this Agreement; and
      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 5.3 to 5.8 of this Agreement.
      3. In this clause 5.8, “sub-contract” means a contract between two or more suppliers, at any stage of remoteness from the Customer 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.
   9. 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. **Premises and equipment**
   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.
   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.
   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.
   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.
   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. 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.
   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.
6. **Staff and Key Personnel**
   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:
      1. refuse admission to the relevant person(s) to the Customer’s premises;
      2. direct the Supplier to end the involvement in the provision of the Services of the relevant person(s); and/or
      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.

* 1. The Supplier shall:
     1. ensure that all Staff are vetted in accordance with the Staff Vetting Procedures;
     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
     3. procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Customer.
  2. Any Key Personnel shall not be released from supplying the Services without the agreement of the Customer, except by reason of long-term sickness, parental leave and termination of employment or other extenuating circumstances.
  3. 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.

1. **Assignment and sub-contracting**
   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.
   2. 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.
   3. 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.
2. **Intellectual Property Rights** 
   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 or the respective owner of such intellectual property rights 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.
   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).
   3. The Supplier hereby grants the Customer:
      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
      2. a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:
         * 1. any intellectual property rights vested in or licensed to the Supplier on the date of the Agreement; and
           2. 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.
   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.
3. **Governance and Records**
   1. The Supplier shall:
      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
      2. submit progress reports to the Customer at the times and in the format specified by the Customer.
   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.
4. **Confidentiality, Transparency and Publicity**
   1. Subject to clause 11.2, each Party shall:
      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
      2. not use or exploit the disclosing Party’s Confidential Information in any way except for the purposes anticipated under the Agreement.
   2. Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:
      1. where disclosure is required by applicable law or by a court of competent jurisdiction;
      2. to its auditors or for the purposes of regulatory requirements;
      3. on a confidential basis, to its professional advisers;
      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;
      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
      6. where the receiving Party is the Customer:
         * 1. on a confidential basis to the employees, agents, consultants and contractors of the Customer;
           2. 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;
           3. to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or
           4. 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.
   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.
   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.
5. **Freedom of Information** 
   1. The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:
      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;
      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;
      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
      4. not respond directly to a Request for Information unless authorised in writing to do so by the Customer.
   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.
   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.
6. **Protection of Personal Data and Security of Data**
   1. The Supplier shall, and shall procure that all Staff shall, comply with any notification requirements under Data Protection Legislation and both Parties shall duly observe all their obligations under Data Protection Legislation which arise in connection with the Agreement.
   2. REPLACED BY ANNEX 6 IN RELATION TO PROTECTION OF PERSONAL DATA
   3. When handling Customer data (whether or not Personal Data), the Supplier shall ensure the security of the data is maintained in line with the security requirements of the Customer as notified to the Supplier from time to time.
7. **Liability** 
   1. The Supplier shall not be responsible for any injury, loss, damage, cost or expense suffered by the Customer if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Agreement.
   2. Subject always to clauses 14.3 and 14.4:
      1. the aggregate liability of the Supplier in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the Charges paid or payable to the Supplier; and
      2. except in the case of claims arising under clauses 9.4 and 18.3, in no event shall the Supplier be liable to the Customer for any:
         * 1. loss of profits;
           2. loss of business;
           3. loss of revenue;
           4. loss of or damage to goodwill;
           5. loss of savings (whether anticipated or otherwise); and/or
           6. any indirect, special or consequential loss or damage.
   3. Nothing in the Agreement shall be construed to limit or exclude either Party's liability for:
      1. death or personal injury caused by its negligence or that of its Staff;
      2. fraud or fraudulent misrepresentation by it or that of its Staff; or
      3. any other matter which, by law, may not be excluded or limited.
   4. The Supplier’s liability under the indemnity in clause 9.4 and 18.3 shall be unlimited.
8. **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 Party affected. 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.

1. **Termination**
   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.
   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:
      1. (without prejudice to clause 16.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;
      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;
      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;
      4. undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;
      5. breaches any of the provisions of clauses 7.2, 11, 12, 13 and 17;
      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 16.2.6) in consequence of debt in any jurisdiction; or
      7. fails to comply with legal obligations in the fields of environmental, social or labour law.
   3. The Supplier shall notify the Customer as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.
   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.
   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, 13, 14, 16.6, 17.4, 18.3, 19 and 20.7 or any other provision of the Agreement that either expressly or by implication has effect after termination.
   6. Upon termination or expiry of the Agreement, the Supplier shall:
      1. give all reasonable assistance to the Customer and any incoming supplier of the Services; and
      2. return all requested documents, information and data to the Customer as soon as reasonably practicable.
2. **Compliance**
   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.
   2. The Supplier shall:
      1. comply with all the Customer’s health and safety measures while on the Customer’s premises; and
      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.
   3. The Supplier shall:
      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
      2. take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.
   4. The Supplier shall supply the Services in accordance with the Customer’s environmental policy as provided to the Supplier from time to time.
   5. The Supplier shall comply with, and shall ensure that its Staff shall comply with, the provisions of:
      1. the Official Secrets Acts 1911 to 1989; and
      2. section 182 of the Finance Act 1989.
3. **Prevention of Fraud and Corruption**
   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.
   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.
   3. If the Supplier or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Customer) the Customer may:
      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
      2. recover in full from the Supplier any other loss sustained by the Customer in consequence of any breach of this clause.
4. **Dispute Resolution**
   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.
   2. If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, 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.
   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.
5. **General**
   1. Each of the Parties represents and warrants to the other that it has full capacity and Customer, 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.
   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.
   3. The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.
   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.
   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.
   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 Customer to make any commitments on the other Party’s behalf.
   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.
   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.
6. **Notices**
   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 21.3, 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:
   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.
   3. Notices under clauses 15 (Force Majeure) and 16 (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 21.1.
7. **Governing Law and Jurisdiction**

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

**ANNEX 2 – PRICE SCHEDULE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Whole-life cost split over financial years:** | | | |
|  | **Capital (CDEL)** | **Resource (RDEL)** | **Annual total** |
| **2022/23** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| **2023/24** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| **2024/25** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| **Whole-life total cost** |  | £5,337,210 | £5,337,210 |

**ANNEX 3 – STATEMENT OF REQUIRE****MENTS**

# PURPOSE

## The Office of Government Property (OGP) wishes to contract the Improvement and Development Agency, part of the Local Government Association (LGA), to work in collaboration with OGP to deliver the One Public Estate (OPE) programme.

# BACKGROUND TO THE CONTRACTING AUTHORITY

## The Office of Government Property (then the Government Property Unit) was established in 2010 within the Cabinet Office. The unit has central oversight over government land and property and works collaboratively across the Civil Service to:

### Create an effective and efficient government estate.

### Provide value for money for the taxpayer.

### Dispose of surplus property in a way that maximises financial return.

### Boost growth and create new homes.

## The OPE programme, run jointly by OGP and the LGA, supports collaboration on land and property initiatives at a local level and helps local authorities take a leading role locally on asset management.

# Background to requirement/OVERVIEW of requirement

## The OPE Programme is a pioneering initiative delivered by OGP in collaboration with the LGA. The programme channels funding and practical and technical support through local authorities to deliver collaborative property-focused projects with central government and other partners. The OGP and LGA collaboration is critical to the programme’s credibility, influence and impact with local government, and supports the development of central government policy that tackles cross-public sector property issues.

## The OPE programme has four core objectives:

### Create economic growth, including new homes and jobs.

### Deliver more integrated and customer-focused services.

### Generate capital receipts.

### Reduce running costs.

## Joint delivery of the programme between OGP and the LGA helps to create an effective way of working between local and central government and the wider public sector. As the representative body of local government], the LGA is the only organisation that has the relevant experience, knowledge and expertise in local government to help deliver the OPE programme.

## Joint delivery of the programme is achieved through a combined, regionally based delivery team, details of which can be found in Schedule A – Team Structure.

## The LGA has an in-depth understanding of the political landscape and challenges of local government that are invaluable to the programme’s successful delivery. The LGA have a trusted and established relationship with all local authorities in England, which provides the credibility to directly manage OPE’s engagement with them. This could not be achieved by OGP working alone and is critical to the delivery of the programme.

## In 2017, OPE entered into a partnership with the Ministry for Housing, Communities and Local Government (MHCLG) now known as the Department for Levelling Up, Housing and Communities (DLUHC) to deliver the £45m Land Release Fund (LRF). The LRF aims to accelerate the release of council land to meet the ambition to release land for new homes. The OPE programme is critical to supporting the LRF programme targets, including monitoring progress and unblocking issues.

## OPE also delivers the Brownfield Land Release Fund (BLRF), a DLUHC-funded capital programme that aims to unlock otherwise unviable local authority land for housing. Together, OPE and the BLRF constitute a coordinated approach to delivering more homes, at pace, through the sale and development of surplus local authority land.

## In May 2021, HMT approved a £100m Business Case to cover delivery of OPE and BLRF programmes in 21-22, 22-23 and 23-24. That included a commitment by DLUHC’s Investment Sub Committee that £2.28m in revenue costs would be paid to the Cabinet Office in 21-22, 22-23 to cover staffing costs for the programme. This covers the entirety of the annual LGA contract and 6 Cabinet Office posts. Funding is expected to be transferred to the Cabinet Office at Supplementary Estimates, subject to business planning (due early April 2022).

## Contract governance is as such: OPE has a Director-chaired programme board, on which sit CO, DLUHC and the LGA for SRO insight and direction. There are quarterly joint Senior Leadership Team meetings between all parties, and a weekly SLT between CO and LGA to discuss and direct programme progress. Day-to-day working between all team members, working towards joint goals and outcomes. Performance reports are presented to the Programme Executive Group (PEG) to provide governance oversight. The Minister for Brexit Opportunities and Efficiency is also updated regularly on programme performance and OPE will be reporting benefits on a quarterly basis to CO Finance and HMT.

## The first year of the Contract will run for 9 months from 1st July 2022 to 31st March 2023. A three-month extension to the 21/22 Contract was approved in February 2022 to mitigate against the LGA working at risk in the first quarter of 22/23 due to delays in contract approval.

## The OGP will hereafter be referred to as ‘the Authority’ and the LGA will hereafter be referred to as ‘the Supplier’.

# definitions

|  |  |
| --- | --- |
| Expression or Acronym | Definition |
| OPE | One Public Estate Programme |
| BLRF | Brownfield Land Release Fund |
| OGP | Office of Government Property (Cabinet Office) |
| LGA | Local Government Association |
| PEG | Programme Executive Group |
| SLT | Senior Leadership Team |

# scope of requirement

## The scope of the Supplier’s contribution sits within the OPE programme, including all aspects of its delivery as outlined in The Requirement (Section 6) in collaboration with the Authority, with a specific responsibility to take the lead on local government aspects.

# The requirement

## The Supplier will work as a blended team with the Authority, provide practical advice, challenge and support to local authorities and public sector partnerships to drive delivery of local OPE and B/LRF programmes and enable them to achieve expected outcomes. This includes the employment of a team (as outlined in Schedule A – Team Structure) of Regional Programme Managers to provide support and challenge to local OPE partnerships.

## The Supplier shall contribute to influence change across the public sector assets landscape, including participating in seminars, workshops and conferences. The Supplier will engage in discussions on new tools for local authorities, public sector bodies and with experts to develop proposals for new offers throughout the programme, e.g. investment.

## The Supplier shall work as a blended team with the Authority to support OPE partnerships. They will facilitate dialogue with, and secure engagement of other key public estate holders in localities for the aim of identifying, developing and delivering OPE projects. This includes delivering the homes this country needs, in particular making the most of surplus land already in public ownership and supporting Local Authorities to release their land.

## The Supplier will be expected to complete the following activities in relation to strategic relationship engagement and management:

### Support local government to maintain robust and sustainable OPE governance arrangements at a senior level (senior directors and chief executives) in all OPE Partnerships, with membership reflecting local area partners.

### Actively seek opportunities to increase the impact and visibility of the programme.

### Broker relationships between local public sector partners and act as neutral mediators in delivery issues.

### Attend OPE Partnership boards.

### Recruit and maintain a skilled programme team representative of regional operational staff, programme leadership and support staff.

## The Supplier shall support delivery and obtain information on land assets and disposal plans using existing OPE partnerships (coverage of 95% of Local Authorities). They will also support effective governance of the programme within OPE partnerships and centrally with the Authority’s programme team.

## The Supplier shall deliver day-to-day management of the programme alongside the Authority’s programme team to develop working relationships with OPE partnerships, enabling the realisation of the benefits to wider place-based working. This will include providing ongoing programme intelligence, best practice and shared learning for local government to help the OPE programme support all partnerships. This will include the following tasks:

### Support benefits delivery through engagement with and assistance provided to OPE Partnerships and project owners.

### Assistance to unblock barriers to delivery and partnership working.

### Seek and support innovative solutions to challenges in delivering OPE funded projects.

### Sharing programme best practice.

### Enabling local social value to be achieved through economic growth.

### Developing and maintaining a library of case studies, best practice examples and scope and deliver an effective communication and engagement strategy.

### Facilitating opportunities workshops.

## The Supplier shall administer the local partnerships application process for OPE funding, bid assessment process within the OPE team and other government departments. They will also award funding to successful projects and provide detailed feedback to each bidding partnership. This will include the following tasks:

### Support the launch and delivery of funding rounds and distribution of subsequent funding documentation; maximising the allocation of available funding.

### Promoting the programme and encouraging acceptable bids from partnerships.

### Support OPE Partnerships to submit accurate proposals and meet the pre-selection criteria.

### Obtain and accurately collate bank details for each partnership awarded funding.

### Distributing and collating project delivery plans and agreements with Partnerships.

## The Supplier shall support the OPE programme reporting procedures and provide ongoing monitoring and management of projects and partnerships to realise benefits. They will assemble and share relevant data on land and property, including local partner asset mapping. This will include the following activities:

### Support the completion of OPE’s tri-annual reporting process and maintenance of the quality of the programme data set, by contributing to the delivery of dashboards and reports to PEG.

### Providing support to OPE Partnerships to complete tri-annual reports.

### Ensuring accurate and quality data is collated and input into the Mastersheet.

### Identify and raise any risks to the delivery of reports to PEG.

### Compile accurate content for inclusion in PEG papers.

### Collation of appropriate evidence from Partnerships to enable the validation of benefits tri-annually.

## The Supplier is expected to effectively deliver management of individual project and partnership programme risk through the development of agreed risk processes and implementation of prioritised approaches to delivery to minimise risk. This will include the following activities:

### Identification and monitoring of individual project risks and OPE Partnership risks. Consideration of programme level risks. Development and implementation of activity to mitigate risks.

### Identifying, assessing, addressing, reporting, escalating and reviewing risks.

## The Supplier will provide robust change management by providing early warning of proposed changes that will affect programme delivery. This will include the following activities:

### Support effective management of changes that will affect programme delivery.

### Communicating the change request process to OPE Partnerships.

### Supporting partnerships to identify the need for change requests.

### Retain and support a change control log.

### Assess change requests from partnerships and negotiate acceptable changes.

### Provide change request recommendations to SLT/PEG.

## They should ensure that projects are effectively evaluated including learning reviews and project closure processes including:

### Support the development of an effective Project Closure and Evaluation process.

### Contributing to the Project Closure and Evaluation Strategy.

### Contributing to the development of the process for the completion of project learning reviews.

## The Supplier shall enable and support programme growth by seeking innovative approaches to programme investment. This will include the following activities:

### Enable and support programme growth through innovative approaches to programme investment.

### Identifying and developing alternative funding models with partnerships.

### Support partnership OPE bids to include sustainable grant proposals.

### Identify sustainable and innovative OPE activity and share best practices.

## They will contribute to the programme’s strategic communications, by developing a communications plan, identifying opportunities to promote the programme and through having a presence at events. This will include the following activities:

### Increase the profile of OPE and B/LRF.

### Identifying opportunities to promote OPE and B/LRF to relevant stakeholders.

### Promote OPE and B/LRF to relevant stakeholders.

### Support the development of a library of case studies to reflect the breadth of the programme.

## The Authority and the Supplier are jointly responsible for the delivery of the OPE programme. This means at any point, either party may take more of a lead in facilitating OPE relationships.

## The Authority and the Supplier will work in collaboration to identify who is best suited to support the activity required. This could include the Authority leading the development of links between OPE and Government Departments or the Supplier engaging local authorities with sensitive or difficult messages.

## The Authority are responsible for agreeing funding awards, authorising spend and making grant payments, in line with Cabinet Office policies and procedures.

# key milestones and Deliverables

## The following Contract milestones/deliverables shall apply:

|  |  |  |
| --- | --- | --- |
| Milestone/ Deliverable | Description | Timeframe or delivery date |
| 1 | Support the delivery of £930m capital receipts, £195m running cost savings, 60,000 jobs and land released for 41,500 homes from OPE investment | March 2024 |
| 2 | Working with the Authority, DLUHC and Homes England to help deliver the aims of the Brownfield/Land Release Fund programme, and help to meet the government's key housing ambition to build 300,000 new homes a year. | March 2023 |
| 3 | Provide support to enable OPE partnerships to report benefits accurately and with acceptable supporting evidence | Tri-annually |
| 4 | Design and successfully deliver the Brownfield Land Release Fund 2 programme across three funding rounds (1 per year) | March 2025 |
| 5 | Ensure that the LGA meets Cabinet Office governance requirement e.g., PEG | Quarterly |
| 6 | Ensure that the LGA’s capacity remains at a minimum of 80% throughout the year | March 2023 |

# 

# MANAGEMENT INFORMATION/reporting

## In collaboration with the Authority, the Supplier will support the process of monitoring and reporting on OPE project delivery throughout the programme. This involves the Regional Programme Managers from both parties monitoring progress at a local level and reporting to the central programme team.

## The OPE programme should support local authorities to robustly forecast and track benefits, formally collecting and collating data to report progress against capital receipts, running cost savings, jobs created and land released for housing.

## The OPE, B/LRF and DLUHC senior team meet weekly to oversee and guide the programme’s strategic direction and implementation, informed by the reporting data collated.

## The Programme Management Office, involving the Authority, the Supplier and DLUHC staff, also meets weekly to manage the day-to-day running of the programme as well as risks and issues.

# volumes

## The volume of work to be undertaken is likely to increase year on year. With the commencement of the future programmes, such as BLRF2 and OPE Phase 10, which we expect to launch in 2022/23, subject to approvals. It is anticipated that this will result in a larger number of projects to oversee and support, as well as a larger number of funding applications to assess than in previous years.

## Funding rounds may also differ in timing each year and are dependent upon approvals.

## Volumes of work will be reviewed on an annual basis (31st March annually) to enable effective workload planning for OPE programme delivery.

# continuous improvement

## Through the Programme Management Office, the Authority and the Supplier will continually review OPE and B/LRF systems, processes and programme delivery to ensure the programmes continue to be delivered effectively and efficiently, and opportunities to improve are identified and implemented.

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

## The Supplier should present new ways of working to the Authority during quarterly Contract review meetings.

## Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.

# Sustainability

## The OPE programme is encouraging partnerships to move to a more self-sustaining funding model, embedding a long-term way of working. To support this, OPE will look to diversify its funding streams, including private sector investment in local projects.

## The OPE programme team will encourage self-funding of OPE projects, the take-up of sustainable grant funding and help to seek suitable match funding from other partners.

## OPE will support partnerships to develop proposals for OPE funding maximising local and self-investment in projects, enabling place-based working.

## The Supplier will support activity to engage private sector stakeholders and explore investment and innovation opportunities.

# quality

## No specific quality accreditations are deemed appropriate for this requirement.

## The Supplier will ensure high-quality services are delivered through the OPE programme as outlined in Section 14. Staff and Customer Service.

## Further quality requirements will be monitored through Section 15 Service Levels and Performance - Key Performance Indicators.

# PRICE

* 1. The price for the Supplier’s services will not exceed **REDACTED TEXT under FOIA Section 43 Commercial Interests** in 2022/23, and **REDACTED TEXT under FOIA Section 43 Commercial Interests** per annum in each of 23/24 on a time and materials basis. This will cover staff costs and related expenses necessary for the delivery of the programme.

## An overhead of no more than **REDACTED TEXT under FOIA Section 43 Commercial Interests**% can be charged in addition to staff costs. This is to be reflected within the rate provided for each role.

## Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

# STAFF AND CUSTOMER SERVICE

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

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

## The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

# service levels and performance

## The Authority will manage the delivery of agreed service levels for programme process management, performance management and change controls.

## The Authority will measure the quality of the delivery by monitoring key performance indicators that contribute towards the achievement of the OPE objectives to create economic growth through new homes and jobs, deliver more integrated, customer-focused services and through generating efficiencies, resulting from capital receipts and reduced running costs.

## The Authority will measure the quality of the Supplier’s delivery by:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **KPI** | **Service Area** | **Description** | **Dependencies** | **Target** | **Evidence Required** |
| **1** | **Strategic Relationship Engagement and Management (Performance)** | Engage with and maintain strategic relationships with Cabinet Office (CO) and Department for Levelling Up and Housing (DLUHC) |  | Weekly SLT meetings Programme Director meetings  Regular DLUHC catch-ups | Board papers SLT minutes  Secretariat responsibilities fulfilled Attendance of meetings |
|  |  | Quarterly two-way engagement with all Local Authorities that are part of the programme. |  | Regional Teams attending Partnership Board meetings Site visits, Deep Dives Regional Networks events | Confirmation from director. Screen grabs of team calendars. T&S Datasheet showing travel. OPE Partnership Board minutes.  Evidence of site visits/events Information from board meetings/minutes |
|  |  | Provide insight to Local Authority priorities through regular engagement and attendance at partnership meetings. | CO RPMs links with lead Departments provides CG insight | Qualitative intelligence for Regional Reviews 3 x pa and pipeline / fund development | Regional Review presentations and minutes from meetings. Regional Strategies/plans. |
| **2** | **Effective administration of Funding Rounds (Performance)** | One Public Estate (OPE) Funding - LGA to provide timely and effective inputs and sector insights to the design, development & administration of the OPE fund within the spending review period to deliver ministerial objectives through ensuring LGA inputs to activity within timelines have been met and through the accuracy of information provided to the CO. LGA inputs have a focus on fund design, sector engagement plus assessment and administration processes. | Significant dependencies within timelines relating to CO and DLUHC led activities, for example securing ISC, HMT, Ministerial sign offs, and in terms of grid slots and communications planning. And, in relation to ministerial approvals of award recommendations and announcement communications.  CO internal processes for fund approvals. | Delivery of fund design, products and processes to agreed timeline | Evidence of and successful delivery of OPE in 22/23 |
|  |  | Brownfield Release Land (BLRF) Funding - LGA to provide timely and effective inputs and sector insights to the design, development & administration of the BLRF fund within the spending review period to deliver ministerial objectives through ensuring LGA inputs to activity within timelines have been met and through the accuracy of information provided to the CO. LGA inputs have a focus on fund design, sector engagement plus assessment and administration processes. | Significant dependencies within timelines relating to CO and DLUHC led activities, for example securing ISC, HMT, Ministerial sign offs, and in terms of grid slots and communications planning. And, in relation to ministerial approvals of award recommendations and announcement communications. Department of Levelling Up, Housing and Communities (DLUHC) internal processes for fund approvals. | Delivery of fund design, products and processes to agreed timeline | Evidence of and successful delivery of the BLRF in 22/23 |
|  |  | Other Funding - Successful design, development & administration of any other agreed fund within the spending review period to deliver ministerial objectives through ensuring timelines have been met and through the accuracy of information provided to the CO (and other Government departments as appropriate). | Subject to LGA and CO agreement around capacity and priority: if OPE and LRF funds are in design and administration, capacity to develop any further funding programmes may be limited. Government department internal processes for fund approvals. | Delivery of Fund Design & products to agreed timeline |  |
| **3** | **Governance and Decision Making (Performance)** | Fully engage in the OPE programme Governance, ensuring recommendations are made based upon accurate and robust evidence. | CO contribution to governance and decision making | Involvement of Programme Director, Programme Manager, or Senior Partnerships Manager at any PEG, JSLT or SLT meeting. | Confirmation from Programme Director. Agendas and Minutes of PEG/JSLT/SLT meetings |
|  |  | To monitor, report, and propose mitigations regarding programme risks related to partnerships and projects, and LGA contract activity, through the effective operation of the agreed risk management strategy | Approval of Risk Management Strategy. Ability to manage programme risks dependent on CO factors (e.g. CO resourcing, CO financing limitations etc) | Reported to SLT on the back on triannual reporting | Risk log maintained Escalation evidenced through SLT and PEG |
|  |  | To provide SROs (and SLTs) with timely and accurate performance information, based upon the tri-annual reports, regional reviews and other appropriate sources of data and intelligence. | Data held on CO administered Google Drive system | Accurate reporting of outcomes from triannual reporting and regional reviews | Evidence of reporting from SLT and data logged |
| **4** | **Programme Sustainability (Social Value)** | Contribute to the sustainable approach/strategy for the OPE programme through management of partnerships, stakeholders and process, otherwise manage through the change process. |  | Ensuring the return of grants in Q1-3 only Ensuring RAG ratings for returns are updated quarterly Reporting change requests | Evidence of grants returns in Q1-3 Evidence of up to date RAG ratings Up to date change log |
|  |  | Contribute to the OPE's commercial strategy through involvement in quarterly review meetings (development & delivery). | Recruitment of Head to Commercial to CO OPE team  Commercial Strategy |  |  |
|  |  | Contribute to the strategy and project intentions of the OPE programme ensuring government and local social value priorities are reflected in the LGA's inputs to the programme (sector intelligence, advice, recommendations, programme information, process design etc). |  | Ensure LGA advice inputs to OPE programme strategy & fund design responds to priorities to deliver against strategic objectives, such as in the Government Property Strategy, Levelling Up |  |
| **5** | **Strategic Communications (Performance)** | Develop, maintain and deliver an OPE communications strategythrough completion of the strategy for 22/23 and delivery of the actions. |  | Design, development and completion of the strategy for 22/23 and delivery of the actions. | Evidence of delivered actions e.g. website, comms strategy and events |
|  |  | Regular liaison with comms leads in the CO, minimum monthly, to ensure a joined-up approach to all OPE comms. |  | Monthly meetings | Confirmation from CO  Actions logged |
|  |  | Annual communications review with CO to review communications activities and outcomes and inform the 23/24 strategy. |  | Annual reviews | Evidence from outcome of annual reviews |
| **6** | **Cost of Delivery (Performance)** | Deliver OPE within the agreed budget envelope for 22/23. |  | Delivery to forecasted budget | Evidence of forecasted budget being met |
|  |  | Accurate forecasting and reporting of actuals every period (month). | CO & LGA finance team & processes | Actuals will be provided monthly | Confirmation from CO  Accurate forecasting |
| **7** | **Resourcing (Performance)** | Operate with sufficient resources (people) to deliver the programme objectives, including funding rounds and reporting | Contract Funding, CO resource levels impact on LGA resourcing when LGA required to cover more | No more than 20% vacancies across the year | Staffing levels/ data (quarterly) Evidence of 80% resourcing |

## Performance will be monitored on a quarterly basis throughout the duration of the contract to ensure that key milestones and SLA’s are adhered to.

# Security and CONFIDENTIALITY requirements

## The Supplier’s staff will undertake baseline checks as standard to work in **REDACTED TEXT UNDER FOIA SECTION 40 PERSONAL INFORMATION** Road and to share data on OPE.

## The Supplier shall be expected to work in line with the Authority’s IT policy included in Schedule B Security Management.

# payment AND INVOICING

## Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

## Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

## Invoices should be submitted to: **REDACTED TEXT UNDER FOIA SECTION 40 PERSONAL INFORMATION**

## Invoices should detail the specific purchase order details provided by The Authority; the Supplier should note that invoices not detailing the correct purchase order number may be rejected for payment. The invoices should appropriately apply VAT.

## Payment will be made quarterly, in arrears.

## Expenses for travel and subsistence outside the base location will be charged at cost and evidenced by the supplier as requested by the Authority. Expenses will be reasonable and aligned to the Authority's expenses policy, Schedule C Subsistence Rates.

## Any changes to the team structure that would lead to an increase in costs, must be approved by the Programme Director within OGP, prior to any changes taking place.

# CONTRACT MANAGEMENT

## The Supplier will nominate an appropriate senior member of staff to attend quarterly contract review meetings with the Authorities OPE Contract Manager.

## Both parties will schedule an annual review of the contract and requirements and make appropriate updates as deemed necessary for programme delivery.

## Attendance at Contract Review meetings shall be at the Supplier’s own expense.

## Any escalation throughout the programme will be raised with The Authorities Programme Director.

# Location

## The location of the Services will be carried out at **REDACTED TEXT UNDER FOIA SECTION 40 PERSONAL INFORMATION** which will be classed as the base location, and other places of work, most notably on location with stakeholders.

## The current LGA headquarters is: **REDACTED TEXT UNDER FOIA SECTION 40 PERSONAL INFORMATION**

**ANNEX 4 – SUPPLIERS RESPONSE**

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

**ANNEX 5 – CLARIFICATIONS**

**Not Applicable**

**ANNEX 6 – ADDITIONAL TERMS & CONDITIONS**

1. Data Protection

* 1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer and the Supplier are Joint Controllers. This is because the Customer and Supplier are both playing a role in deciding how Personal Data is processed to provide the Services.
  2. The Customer and Supplier agree, in accordance with Article 26 UK GDPR, to have a Joint Controller agreement that sets out their intentions in respect of the jointly processed Personal Data.

**ANNEX 7 – CHANGE CONTROL FORMS**

|  |  |  |  |
| --- | --- | --- | --- |
| CHANGE CONTROL NOTICE (CCN) | | | |
| Contract Title: | Contract for the Provision of OPE Managed Services Contract (The Contract) | | |
| Contract Reference: | CCCC22A09 | Contract Change Number: |  |
| Date CCN issued: |  | Date Change Effective from: |  |
| Between: The Cabinet Office (The Customer) and Improvement and Development Agency (LGA) (The Supplier)   1. The Contract is varied as follows:   1.1. Insert details of changes to the original Contract.   1. Words and expressions in this Change Control Notice shall have the meanings given to them in the Contract. 2. The Contract, including any previous Contract changes, authorised in writing by both Parties, shall remain effective and unaltered except as amended by this Change Control Notice. | | | |
| Change authorised to proceed by:  (Customer’s representative):      Signature Print Name and Job Title Date | | | |
| Authorised for and on behalf of the Supplier:  Signature Print Name and Job Title Date | | | |
| Authorised for and on behalf of the Customer:  Signature Print Name and Job Title Date | | | |

**SCHEDULE A – TEAM STRUCTURE**

**REDACTED**

**SCHEDULE B – SECURITY MANAGEMENT**

**Definitions**

In this Schedule B (Security Management):

|  |  |
| --- | --- |
| Anti-virus Software” | means software that:  protects the Supplier Information Management System from the possible introduction of Malicious Software; scans for and identifies possible Malicious Software in the Supplier Information Management System; if Malicious Software is detected in the Supplier Information Management System, so far as possible:   * prevents the harmful effects of the Malicious Software; and * removes the Malicious Software from the Supplier Information Management System; |
| “Breach of Security” | means the occurrence of:   * + 1. any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement;     2. the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or     3. any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements; | |
| “Buyer Data” | means any:  data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or  Personal Data for which the Buyer is a, or the, Data Controller, that is:   * 1. supplied to the Supplier by or on behalf of the Buyer; or   2. that the Supplier generates, processes, stores or transmits under this Agreement. |
| “Buyer Equipment” | means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System; |
| “Buyer System” | means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services; |
| “Certification Default” | means the occurrence of one or more of the circumstances listed in Paragraph 0; |
| “Certification Rectification Plan” | means the plan referred to in Paragraph (a); |
| “Certification Requirements” | means the information security requirements set out in paragraph 0. |
| “Cyber Essentials” | means the Cyber Essentials certificate issued under the Cyber Essentials Scheme; |
| “Cyber Essentials Plus” | means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme; |
| “Cyber Essentials Scheme” | means the Cyber Essentials scheme operated by the National Cyber Security Centre; |
| “End-user Device” | means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services. |
| “HMG Baseline Personnel Security Standard” | means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 (<https://assets.publishing.service.gov.uk> /government/uploads/system/uploads/attachment data/file/714002/ HMG\_Baseline\_Personnel\_Security\_Standard\_-\_May\_2018.pdf), as that document is updated from time to time; |
| “Malicious Software” | means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations; |
| “NCSC Cloud Security Principles” | means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/ implementing-the-cloud-security-principles. |
| “NCSC Device Guidance” | means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance; |
| “Privileged User” | means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges; |
| “Process” | means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data; |
| “Prohibited Activity” | means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice; |
| “Prohibition Notice” | means a notice issued under paragraph 1.3 of Annex 1. |
| “Relevant Certifications” | means those certifications specified in Paragraph 0; |
| “Relevant Convictions” | means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), driving offences, offences against property, drugs, alcohol, public order offences or any other offences relevant to Services as the Buyer may specify; |
| “Security Management Plan” | means the document prepared in accordance with the requirements of Paragraph 0 |
| “Sites” | means any premises:   * + 1. from or at which:   the Services are (or are to be) provided; or  the Supplier manages, organises or otherwise directs the provision or the use of the Services; or   * + 1. where:   any part of the Supplier Information Management System is situated; or  any physical interface with the Buyer System takes place; |
| “Standard Contractual Clauses” | means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area; |
| “Supplier Information Management System” | means:   * + 1. those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; and     2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); |
| “Sub-contractor Personnel” | means:   * + 1. any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and     2. engaged in or likely to be engaged in:        1. the performance or management of the Services;        2. or the provision of facilities or services that are necessary for the provision of the Services. |
| “Supplier Personnel” | means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Agreement; |
| “UKAS” | means the United Kingdom Accreditation Service; |

**Introduction**

* 1. This Schedule B (Security Management) sets out:
     1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Buyer Data, the Services and the Supplier Information Management System;
     2. the assessment of this Agreement as either a:
        1. Standard consultancy agreement; or
        2. Higher-risk consultancy agreement,

in Paragraph 0;

* + 1. the Buyer’s access to the Supplier Personnel and Supplier Information Management System, in Paragraph 4;
    2. the Certification Requirements, in Paragraph 0;
    3. the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in Paragraph 0;
    4. the security requirements with which the Supplier must comply in Annex A;
    5. the security requirements applicable to Sub-contractors in Annex A.

**Principles of Security**

* 1. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:
     1. the Sites;
     2. the Services; and
     3. the Supplier’s Information Management System.
  2. Notwithstanding the involvement of the Buyer in the assurance of the Supplier Information Management System, the Supplier remains responsible for:
     1. the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors; and
     2. the security of the Supplier Information Management System.
  3. The Supplier shall:
     1. comply with the security requirements in Annex 1; and
     2. ensure that each Sub-contractor that Processes Buyer Data complies with the Sub-contractor security requirements in Annex 2.
  4. Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

**Buyer Risk Assessment**

* 1. The Buyer has assessed this Agreement as

☑ A standard consultancy agreement;

□ A higher-risk consultancy agreement.

**Access to Supplier Personnel and Supplier Information Management System**

* 1. The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:
     1. access to the Supplier Personnel;
     2. access to the Information Management System to audit the Supplier and its Sub-contractors’ compliance with this Agreement; and
     3. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

* 1. The Supplier must provide the access required by the Buyer in accordance with Paragraph 0 within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

**Certification Requirements**

* 1. The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:
     1. In the case of a standard consultancy agreement:

□ Cyber Essentials Plus;

☑ Cyber Essentials; or

* + 1. In the case of a higher-risk consultancy agreement:
       1. ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2013; and
       2. Cyber Essentials Plus (the “**Relevant Certifications**”).
  1. Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.
  2. The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:
     1. Currently in effect;
     2. Relate to the full scope of the Supplier Information System; and
     3. Are not subject to any condition that may impact the provision of the Services.
  3. The Supplier must notify the Buyer promptly, any in any event within three (3) Working Days of becoming aware that:
     1. A Relevant Certification has been revoked or cancelled by the body that awarded it;
     2. A Relevant Certification expired and has not been renewed by the Supplier;
     3. A Relevant Certification no longer applies to the full scope of the Supplier Information Management System or
     4. The body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”)
  4. Where the Supplier has notified the Buyer of a Certification Default under Paragraph 0:
     1. the Supplier must, within 10 working Days of the date in which the Supplier provided notice under Paragraph 0 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Supplier setting out:
        1. full details of the Certification Default, including a root cause analysis;
        2. the actual and anticipated effects of the Certification Default;
        3. the steps the Supplier will take to remedy the Certification Default;
     2. the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
     3. If the Buyer rejects the Certification Rectification Plan, the Buyer must within 5 Working Days of the date of the rejection submit a revised Certification Rectification Plan and Paragraph (b) will apply to the re-submitted plan;
     4. The rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;
     5. If the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

**Security Management Plan**

*Preparation of Security Management Plan*

* 1. This Paragraph 0 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
  2. The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule B (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.
  3. The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:
     1. an assessment of the Supplier Information Management System against the requirements of this Schedule B (Security Management), including the Annexes;
     2. the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and
     3. the following information in respect of each Sub-contractor:
        1. the Sub-contractor’s:
           1. Legal name;
           2. Trading name (if any);
           3. Registration details (where the Sub-contractor is not an individual);
        2. the Sites used by the Sub-contractor;
        3. the Buyer Data Processed by the Sub-contractor;
        4. the Processing that the Sub-contractor will undertake in respect of the Buyer Data;
        5. the measures the Sub-contractor has in place to comply with the requirements of this Schedule B (Security Management).
  4. The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:
     1. an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or
     2. a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.
  5. If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

*Updating Security Management Plan*

* 1. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this Paragraph.

*Monitoring*

* 1. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
     1. a significant change to the components or architecture of the Supplier Information Management System;
     2. a new risk to the components or architecture of the Supplier Information Management System;
     3. a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;
     4. a change in the threat profile;
     5. a significant change to any risk component;
     6. a significant change in the quantity of Personal Data held within the Service;
     7. a proposal to change any of the Sites from which any part of the Services are provided; and/or
     8. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.
  2. Within 10 Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

**ANNEX A: SECURITY REQUIREMENTS**

1. **Location**
   1. Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or process Buyer Data either:
      1. In the United Kingdom;
      2. The European Economic Area; or
      3. In a facility operated by an entity where:
         1. The entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable) containing the Standard Contractual Clauses;
         2. The Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the Standard Contractual Clauses;
         3. The Supplier has provided the Buyer with such information as the Buyer requires concerning:
            1. The entity;
            2. The arrangements with the entity; and
            3. The entity’s compliance with the Standard Contractual Clauses; and
         4. The Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.
   2. Where the Supplier cannot comply with one or more of the requirements of paragraph 1:
      1. it must provide the Buyer with such information as the Buyer requests concerning the security controls in places at the relevant location or locations; and
      2. the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
      3. if the Buyer does not grant permission to use that location or those locations, the Supplier must cease to store, access or process Buyer Data at that location or those locations within such period as the Buyer may specify.
   3. The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Buyer Data as specified in the notice (a “**Prohibited Activity**”).
      1. in any particular country or group of countries;
      2. in or using facilities operated by any particular entity or group of entities; or
      3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (a “**Prohibition Notice**”).
   4. Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.
2. **Vetting, Training and Staff Access**

*Vetting before performing or managing Services*

* 1. The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:
     1. That individual has passed the security checks listed in paragraph 2.2; or
     2. The Buyer has given prior written permission for a named individual to perform a specific role.
  2. For the purposes of paragraph 2.1, the security checks are:
     1. The checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
        1. The individual’s identity;
        2. The individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
        3. The individual’s previous employment history; and
        4. That the individual has no Relevant Convictions;
     2. National security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
     3. Such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

*Annual training*

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:
     1. General training concerning security and data handling; and
     2. Phishing, including the dangers from ransomware and other malware;

*Staff access*

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
  2. The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.
  3. Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel’s access to the Buyer Data or part of that Buyer Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

*Exception for certain Sub-contractors*

* 1. Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:
     1. As soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
     2. Provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Buyer reasonably requires; and
     3. Comply, at the Supplier’s cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

1. **Security Testing**
   1. This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

**Note**: the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.

* 1. The Supplier must, at the Buyer’s option, before providing the Services and when reasonably requested by the Buyer, either:
     1. Conduct security testing of the Supplier Information Management System by:
        1. engaging a CHECK Service Provider or a CREST Service Provider;
        2. designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and
        3. providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within 10 Working Days of its receipt by the Supplier; or
     2. Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer’s request or the Effective Date (as appropriate), including:
        1. the parts of the Supplier Information Management System tested;
        2. a full, unedited and unredacted copy of the testing report; and
        3. the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and
        4. the Supplier’s progress in implementing that remediation plan.
  2. The Supplier must remediate any vulnerabilities classified as “medium” or above in the security testing:
     1. before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;
     2. where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:
        1. by the date agreed with the Buyer; or
        2. where no such agreement is reached:
           1. within 5 Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;
           2. within 1 month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and
           3. within 3 months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.

1. **End-user Devices**
   1. The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:
      1. the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
      2. users must authenticate before gaining access;
      3. all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;
      4. the End-under Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
      5. the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data;
      6. the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;
      7. all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2013 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
   2. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
   3. Where there any conflict between the requirements of this Schedule B (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
2. **Encryption**
   1. Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
      1. When stored at any time when no operation is being performed on it; and
      2. When transmitted.
   2. Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:
      1. immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
      2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
      3. provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
   3. The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
   4. This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

* + 1. The subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
    2. The protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.
  1. Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.

1. **Access Control**
   1. The Supplier must, and must ensure that all Sub-contractors:
      1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
      2. require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
      3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
      4. maintain records detailing each person’s access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
   2. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
      1. are accessible only from dedicated End-user Devices;
      2. are configured so that those accounts can only be use for system administration tasks;
      3. require passwords with high complexity that are changed regularly;
      4. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.
   3. The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.
   4. The Supplier must, and must ensure that all Sub-contractors:
      1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
      2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.
2. **Malicious Software**
   1. The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
   2. The Supplier shall ensure that such Anti-virus Software:
      1. is configured to perform automatic software and definition updates;
      2. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
      3. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
   3. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
   4. Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 7.3 shall be borne by the parties as follows:
      1. by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
      2. by the Buyer, in any other circumstance.
3. **Breach of Security**
   1. If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.
   2. The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:
      1. minimise the extent of actual or potential harm caused by such Breach of Security;
      2. remedy such Breach of Security to the extent possible;
      3. apply a tested mitigation against any such Breach of Security; and
      4. prevent a further Breach of Security in the future which exploits the same root cause failure;
   3. As soon as reasonably practicable and, in any event, within 5 Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
   4. The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.
4. **Sub-contractors**
   1. The Supplier must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer’s request.
5. **Third-party Software**
   1. The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Progress the Buyer Data greater than those rights strictly necessary for the use of the software.
6. **Deletion of Buyer Data**
   1. The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer and using a deletion method agreed by the Buyer.

**SCHEDULE C – SUBSISTENCE RATES**

**Mileage**

**Private Vehicle Mileage**

The LGA reimburse within HMRC advisory mileage rates for all private car mileage, as follows:

|  |  |  |
| --- | --- | --- |
| **Vehicle type** | **Mileage** | **HMRC**  **Rate** |
| Motor car or van (all  engine sizes) | Per mile first 10,000 business miles | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| Per mile over 10,000 business miles | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| Motor cycle | All business miles | **REDACTED TEXT under FOIA Section 43 Commercial Interests**  **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| Bicycle | All business miles |  |

**Subsistence**

**Day meetings**

Breakfast/beverages Up to **REDACTED TEXT under FOIA Section 43 Commercial Interests**

Evening meal Up to **REDACTED TEXT under FOIA Section 43 Commercial Interests**

**Overnight stays**

Accommodation

|  |  |
| --- | --- |
| **Hotel location** | **Maximum agreed rate** |
| London | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |
| Outside London | **REDACTED TEXT under FOIA Section 43 Commercial Interests** |

Meals and drinks not included in room rate or provided:

Up to **REDACTED TEXT under FOIA Section 43 Commercial Interests**

total per night at meeting/event venue

**Hospitality**

External meeting/pre-meeting:

Up to **REDACTED TEXT under FOIA Section 43 Commercial Interests**

per head

**Set Up Costs**

Maximum home working set-up allowance:

**REDACTED TEXT under FOIA Section 43 Commercial Interests**

(one off payment)

**Expenses Forecast for Initial Contract Term**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| July | August | September | October | November | December | January | February | March |
| REDACTED TEXT under FOIA Section 43 Commercial Interests | | | | | | | | |