**Terms and Conditions**

**CONTRACT FOR WOMENS SUFFRAGE GRANT SCHEME ADMINISTRATOR**

THIS CONTRACT IS DATED ..\*\*\*Insert Date, in manuscript, the Department Signed the Contract Here\*\*\*

Parties

1) **The Secretary of State for Education whose Head Office is at Sanctuary Buildings, Great Smith Street, London, SW1P 3BT acting as part of the Crown (“the Department”);**

and

2) **Ecorys UK Private Limited Company 01650169**

whose registered office is at

Albert House Quay Place, 92-93 Edward Street, Birmingham, B1 2RA

(“the Contractor”)

|  |  |
| --- | --- |
| "Affiliate" | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| “Central Government Body”“the Contract Manager” | means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:(a) Government Department;(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);(c) Non-Ministerial Department; or(d) Executive Agency;Kris MacNaughton, Governments Equality Office/Department of Education, Sanctuary Buildings, Great Smith Street, London, SW1P 3BT |
| "Contractor Personnel" | all employees, agents, Contractors and contractors of the Contractor and/or of any Sub-contractor; |
| “the Contractors Contract Manager | **Rachel Brackwell** |
|  “Confidential Information” | the Department's Confidential Information and/or the Contractor's Confidential Information; |
| "Contracting Department" | any contracting Department as defined in Regulation 5(2) of the Public Contracts (Works, Services and Supply) (Amendment) Regulations 2000 other than the Department; |
| "Contractor Personnel" | all employees, agents, consultants and contractors of the Contractor and/or of any Sub-contractor; |
| "Control" | means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and **"Controls"** and **"Controlled"** shall be interpreted accordingly; |
| **“**Crown” | means Queen Elizabeth II and any successor |
| "Crown Body" | any department, office or agency of the Crown; |
| "Department’s Confidential Information" | all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and suppliers of the Department, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered to be confidential; |
| "Environmental Information Regulations" | the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations; |
| "FOIA" | the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation; |
| “Her Majesty's Government” | means the duly elected Government for the time being during the reign of Her Majesty and/or any department, committee, office, servant or officer of such Government |
| "Information" | has the meaning given under section 84 of the Freedom of Information Act 2000;  |
| "Personal Data" | shall have the same meaning as set out in the Data Protection Act 1998; |
| “Property”  | means the property, other than real property, issued or made available to the Contractor by the Client in connection with the Contract. |
| “Regulatory Bodies” | those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Department and **"Regulatory Body"** shall be construed accordingly. |
| "Request for Information" | a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations; |
| "SME" | means a micro, small or medium-sized enterprise defined in accordance with the European Commission Recommendation 2003/361/EC and any subsequent revisions. |
| "Sub-contractor" | the third party with whom the Contractor enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents; |
| "Working Day" | any day other than a Saturday, Sunday or public holiday in England and Wales. |

**1.2** References to “Contract” mean this contract (and include the Schedules). References to “Clauses” and “Schedules” mean clauses of and schedules to this Contract. The provisions of the Schedules shall be binding on the parties as if set out in full in this Contract.

**1.3** Reference to the singular include the plural and vice versa and references to any gender include both genders. References to a person include any individual, firm, unincorporated association or body corporate.

**2 Commencement and Continuation**

 The Contractor shall commence the Services on *20 November 2017* and, subject to Clause 10.1 shall complete the Services on or before *31 March 2019*

**3 Contractor's Obligations**

**3.1** The Contractor shall promptly and efficiently complete the Services in accordance with the provisions set out in Schedule 1 and the special conditions set out in Schedule 3. Where there is any conflict between the terms of this Contract and the special conditions set out in Schedule 3, the special conditions shall prevail.

**3.2** The Contractor shall comply with the accounting and information provisions of Schedule 4.

**3.3** The Contractor shall comply with all statutory provisions including all prior and subsequent enactments, amendments and substitutions relating to that provision and to any regulations made under it.

**4 Departments Obligations**

 The Department will comply with the payment provisions of Schedule 4 provided that the Department has received full and accurate information and documentation as required by Schedule 4 to be submitted by the Contractor for work completed to the satisfaction of the Department.

**5 Changes to the Department's Requirements**

**5.1** The Department shall notify the Contractor of any material change to the Department's requirement under this Contract.

**5.2** The Contractor shall use its best endeavours to accommodate any changes to the needs and requirements of the Department provided that it shall be entitled to payment for any additional costs it incurs as a result of any such changes. The amount of such additional costs to be agreed between the parties in writing.

**6 Management**

**6.1** The Contractor shall promptly comply with all reasonable requests or directions of the Contract Manager in respect of the Services.

**6.2** The Contractor shall address any enquiries about procedural or contractual matters in writing to the Contract Manager. Any correspondence relating to this Contract shall quote the reference number set out in the Recitals to this Contract.

**7 Contractor's Employees and Sub-Contractors**

**7.1** Where the Contractor enters into a contract with a supplier or contractor for the purpose of performing its obligations under the Contract (the “**Sub-contractor**”) it shall ensure prompt payment in accordance with this clause 7.1. Unless otherwise agreed by the Department in writing, the Contractor shall ensure that any contract requiring payment to a Sub-contractor shall provide for undisputed sums due to the Sub-contractor to be made within a specified period from the receipt of a valid invoice not exceeding:

7.1.1 10 days, where the Sub-contractor is an SME; or

7.1.2 30 days either, where the sub-contractor is not an SME, or both the Contractor and the Sub-contractor are SMEs,

The Contractor shall comply with such terms and shall provide, at the Department’s request, sufficient evidence to demonstrate compliance.

**7.2** The Department shall be entitled to withhold payment due under clause 7.1 for so long as the Contractor, in the Department’s reasonable opinion, has failed to comply with its obligations to pay any Sub-contractors promptly in accordance with clause 7.1. For the avoidance of doubt the Department shall not be liable to pay any interest or penalty in withholding such payment.

**7.3** The Contractor shall take all reasonable steps to satisfy itself that its employees or sub-contractors (or their employees) are suitable in all respects to perform the Services.

**7.4** The Contractor shall immediately notify the Department if they have any concerns regarding the propriety of any of its sub-contractors in respect of work/services rendered in connection with this Contract.

**7.5** The Contractor, its employees and sub-contractors (or their employees), whilst on Departmental premises, shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time.

**7.6** The Contractor shall ensure the security of all the Property whilst in its possession, during the supply of the Services, in accordance with the Department’s reasonable security requirements as required from time to time.

**8 Copyright**

 Copyright in all reports and other documents and materials arising out of the performance by the Contractor of their duties under this Contract are to be assigned to and shall vest in the Crown absolutely. This condition shall apply during the continuance of this Contract and after its termination howsoever arising.

**9 Warranty and Indemnity**

**9.1** The Contractor warrants to the Department that the obligations of the Contractor under this Contract will be performed by appropriately qualified and trained personnel with reasonable skill, care and diligence and to such high standards of quality as it is reasonable for the Department to expect in all the circumstances. The Department will be relying upon the Contractor's skill, expertise and experience in the performance of the Services and also upon the accuracy of all representations or statements made and the advice given by the Contractor in connection with the performance of the Services and the accuracy of any documents conceived, originated, made or developed by the Contractor as part of this Contract. The Contractor warrants that any goods supplied by the Contractor forming a part of the Services will be of satisfactory quality and fit for their purpose and will be free from defects in design, material and workmanship.

**9.2** Without prejudice to any other remedy, if any part of the Services is not performed in accordance with this Contract then the Department shall be entitled, where appropriate to:

**9.2.1** require the Contractor promptly to re-perform or replace the relevant part of the Services without additional charge to the Department; or

**9.2.2** assess the cost of remedying the failure (“the assessed cost”) and to deduct from any sums due to the Contractor the Assessed Cost for the period that such failure continues.

**9.3** The Contractor shall be liable for and shall indemnify the Department in full against any expense, liability, loss, claim or proceedings arising under statute or at common law in respect of personal injury to or death of any person whomsoever or loss of or damage to property whether belonging to the Department or otherwise arising out of or in the course of or caused by the provision of the Services.

**9.4** The Contractor shall be liable for and shall indemnify the Department against any expense, liability, loss, claim or proceedings arising as a result of or in connection with any breach of the terms of this Contract or otherwise through the default of the Contractor

**9.5** All property of the Contractor whilst on the Department's premises shall be there at the risk of the Contractor and the Department shall accept no liability for any loss or damage howsoever occurring to it.

**9.6** The Contractor shall ensure that it has adequate insurance cover with an insurer of good repute to cover claims under this Contract or any other claims or demands which may be brought or made against it by any person suffering any injury damage or loss in connection with this Contract. The Contractor shall upon request produce to the Department, its policy or policies of insurance, together with the receipt for the payment of the last premium in respect of each policy or produce documentary evidence that the policy or policies are properly maintained.

**10 Termination**

**10.1** This Contract may be terminated by either party giving to the other party at least *2 months*’ notice in writing.

**10.2** In the event of any breach of this Contract by either party, the other party may serve a notice on the party in breach requiring the breach to be remedied within a period specified in the notice which shall be reasonable in all the circumstances. If the breach has not been remedied by the expiry of the specified period, the party not in breach may terminate this Contract with immediate effect by notice in writing.

**10.3** In the event of a material breach of this Contract by either party, the other party may terminate this Contract with immediate effect by notice in writing.

**10.4** This Contract may be terminated by the Department with immediate effect by notice in writing if at any time: -

**10.4.1** the Contractor passes a resolution that it be wound-up or that an application be made for an administration order or the Contractor applies to enter into a voluntary arrangement with its creditors; or

**10.4.2** a receiver, liquidator, administrator, supervisor or administrative receiver be appointed in respect of the Contractor's property, assets or any part thereof; or

**10.4.3** the court orders that the Contractor be wound-up or a receiver of all or any part of the Contractor's assets be appointed; or

**10.4.4** the Contractor is unable to pay its debts in accordance with Section 123 of the Insolvency Act 1986.

**10.4.5** there is a change in the legal or beneficial ownership of 50% or more of the Contractor's share capital issued at the date of this Contract or there is a change in the control of the Contractor, unless the Contractor has previously notified the Department in writing. For the purpose of this Sub-Clause 10.4.5 “control” means the power of a person to secure that the affairs of the Contractor are conducted in accordance with the wishes of that person by means of the holding of shares or the possession of voting power.

**10.4.6** the Contractor is convicted (or being a company, any officers or representatives of the Contractor are convicted) of a criminal offence related to the business or professional conduct

**10.4.7** the Contractor commits (or being a company, any officers or representatives of the Contractor commit) an act of grave misconduct in the course of the business;

**10.4.8** the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil his/their obligations relating to the payment of Social Security contributions;

**10.4.9** the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil his/their obligations relating to payment of taxes;

**10.4.10** the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to disclose any serious misrepresentation in supplying information required by the Department in or pursuant to this Contract.

**10.5** Nothing in this Clause 10 shall affect the coming into, or continuance in force of any provision of this Contract which is expressly or by implication intended to come into force or continue in force upon termination of this Contract

**11 Status of Contractor**

**11.1** In carrying out its obligations under this Contract the Contractor agrees that it will be acting as principal and not as the agent of the Department.

**11.2** The Contractor shall not say or do anything that may lead any other person to believe that the Contractor is acting as the agent of the Department.

**12 Confidentiality**

**12.1** Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this Contract, each party shall:

**12.1.1** treat the other party's Confidential Information as confidential and safeguard it accordingly; and

**12.1.2** not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

**12.2** Clause12 shall not apply to the extent that:

**12.2.1** such disclosure is a requirement of Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA, Code of Practice on Access to Government Information or the Environmental Information Regulations pursuant to Clause 13 (Freedom of Information);

**12.2.2** such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

**12.2.3** such information was obtained from a third party without obligation of confidentiality;

**12.2.4** such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or

**12.2.5** it is independently developed without access to the other party's Confidential Information.

**12.3** The Contractor may only disclose the Department's Confidential Information to the Contractor Personnel who are directly involved in the provision of the Project and who need to know the information, and shall ensure that such Contractor Personnel are aware of and shall comply with these obligations as to confidentiality.

**12.4** The Contractor shall not, and shall procure that the Contractor Personnel do not, use any of the Department's Confidential Information received otherwise than for the purposes of this Contract.

**12.5** The Contractor shall ensure that their employees, servants or such professional advisors or consultants are aware of the Contractor’s obligations under this Contract.

**12.6** Nothing in this Contract shall prevent the Department from disclosing the Contractor's Confidential Information:

**12.6.1** on a confidential basis to any Central Government Body for any proper purpose of the Department or of the relevant Central Government Body;

**12.6.2** to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;

**12.6.3** to the extent that the Department (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;

**12.6.4** on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any of the entities described in Clause 12.6.1 (including any benchmarking organisation) for any purpose relating to or connected with this Contract;

**12.6.5** on a confidential basis for the purpose of the exercise of its rights under this Contract, including audit rights, step-in rights and exit management rights; or

**12.6.6** on a confidential basis to a proposed successor body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Contract.

**12.7** The Department shall use all reasonable endeavours to ensure that any Central Government Body, Contracting Department, employee, third party or Sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to clause 12 is made aware of the Department's obligations of confidentiality.

**12.8** Nothing in this clause 12 shall prevent either party from using any techniques, ideas or know-how gained during the performance of the Contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of Intellectual Property Rights.

**12.9** The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Contract is not Confidential Information. The Department shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.

**12.10** Subject to Clause 12.9, the Contractor hereby gives its consent for the Department to publish the Contract in its entirety, including from time to time agreed changes to the Contract, to the general public.

**12.11** The Department may consult with the Contractor to inform its decision regarding any redactions but the Department shall have the final decision in its absolute discretion.

**12.12** The Contractor shall assist and cooperate with the Department to enable the Department to publish this Contract.

**13 Freedom of Information**

**13.1** The Contractor acknowledges that the Department is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and cooperate with the Department to enable the Department to comply with its information disclosure obligations.

**13.2** The Contractor shall and shall procure that its Sub-contractors shall:

13.2.1 transfer to the Department all Requests for Information that it receives as soon as practicable and in any event within two Working Days of receiving a Request for Information;

13.2.2 provide the Department with a copy of all Information in its possession, or power in the form that the Department requires within five Working Days (or such other period as the Department may specify) of the Department's request; and

13.2.3 provide all necessary assistance as reasonably requested by the Department to enable the Department to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.

**13.3** The Department shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Contract or any other agreement whether any Information is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.

**13.4** In no event shall the Contractor respond directly to a Request for Information unless expressly authorised to do so by the Department.

**13.5** The Contractor acknowledges that (notwithstanding the provisions of Clause 13) the Department may, acting in accordance with the Ministry of Justice’s Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 (**“the Code”**), be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Contractor or the Project:

13.5.1 in certain circumstances without consulting the Contractor; or

13.5.2 following consultation with the Contractor and having taken their views into account;

provided always that where 13.5.1 applies the Department shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Contractor advanced notice, or failing that, to draw the disclosure to the Contractor’s attention after any such disclosure.

**13.6** The Contractor shall ensure that all Information is retained for disclosure and shall permit the Department to inspect such records as requested from time to time.

**14 Access and Information**

 The Contractor shall provide access at all reasonable times to the Department's internal auditors or other duly authorised staff or agents to inspect such documents as the Department considers necessary in connection with this Contract and where appropriate speak to the Contractors employees.

**15 Transfer of Responsibility on Expiry or Termination**

**15.1** The Contractor shall, at no cost to the Department, promptly provide such assistance and comply with such timetable as the Department may reasonably require for the purpose of ensuring an orderly transfer of responsibility upon the expiry or other termination of this Contract. The Department shall be entitled to require the provision of such assistance both prior to and, for a reasonable period of time after the expiry or other termination of this Contract.

**15.2** Such assistance may include (without limitation) the delivery of documents and data in the possession or control of the Contractor which relate to this Contract, including the documents and data, if any, referred to in the Schedule.

**15.3** The Contractor undertakes that it shall not knowingly do or omit to do anything which may adversely affect the ability of the Department to ensure an orderly transfer of responsibility.

**16** **Tax Indemnity**

**16.1** Where the Contractor is liable to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration.

**16.2** Where the Contractor is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration.

**16.3** The Department may, at any time during the term of this contract, ask the Contractor to provide information which demonstrates how the Contractor complies with Clauses 16.1 and 16.2 above or why those Clauses do not apply to it.

**16.4** A request under Clause 16.3 above may specify the information which the Contractor must provide and the period within which that information must be provided.

**16.5** The Department may terminate this contract if-

(a) in the case of a request mentioned in Clause 16.3 above if the Contractor:

(i) fails to provide information in response to the request within a reasonable time, or

(ii) provides information which is inadequate to demonstrate either how the Contractor complies with Clauses 16.1 and 16.2 above or why those Clauses do not apply to it;

(b) in the case of a request mentioned in Clause 16.4 above, the Contractor fails to provide the specified information within the specified period, or

(c) it receives information which demonstrates that, at any time when Clauses 16.1 and 16.2 apply, the Contractor is not complying with those Clauses.

**16.6** The Department may supply any information which it receives under Clause 16.3 to the Commissioners of Her Majesty’s Revenue and Customs for the purpose of the collection and management of revenue for which they are responsible.

**16.7** The Contractor warrants and represents to the Department that it is an independent contractor and, as such, bears sole responsibility for the payment of tax and national insurance contributions which may be found due from it in relation to any payments or arrangements made under this Contract or in relation to any payments made by the Contractor to its officers or employees in connection with this Contract.

**16.8** The Contractor will account to the appropriate authorities for any income tax, national insurance, VAT and all other taxes, liabilities, charges and duties relating to any payments made to the Contractor under this Contract or in relation to any payments made by the Contractor to its officers or employees in connection with this Contract.

**16.9** The Contractor shall indemnify Department against any liability, assessment or claim made by the HM Revenue and Customs or any other relevant authority arising out of the performance by the parties of their obligations under this Contract (other than in respect of employer's secondary national insurance contributions) and any costs, expenses, penalty fine or interest incurred or payable by Department in connection with any such assessment or claim.

**16.10** The Contractor authorises the Department to provide the HM Revenue and Customs and all other departments or agencies of the Government with any information which they may request as to fees and/or expenses paid or due to be paid under this Contract whether or not Department is obliged as a matter of law to comply with such request.

**17 Data Protection Act**

**17.1** With respect to the parties' rights and obligations under this Contract, the parties agree that the Department is the Data Controller and that the Contractor is the Data Processor. For the purposes of this Clause 17, the terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data”, “Process” and “Processing shall have the meaning prescribed under the DPA.

**17.2** The Contractor shall:

17.2.1 Process the Personal Data only in accordance with instructions from the Department (which may be specific instructions or instructions of a general nature as set out in this Contract or as otherwise notified by the Department to the Contractor during the period of the Contract);

17.2.2 Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by law or any Regulatory Body;

17.2.3 Implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

17.2.4 Take reasonable steps to ensure the reliability of any Contractor Personnel who have access to the Personal Data;

17.2.5 Obtain prior written consent from the Department in order to transfer the Personal Data to any Sub-contractors or Affiliates for the provision of the Services;

17.2.6 Ensure that all Contractor Personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Clause17;

17.2.7 Ensure that none of Contractor Personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Department;

17.2.8 Notify the Department within five Working Days if it receives:

17.2.8.1 a request from a Data Subject to have access to that person's Personal Data; or

17.2.8.2 a complaint or request relating to the Department's obligations under the Data Protection Legislation;

17.2.9 Provide the Department with full cooperation and assistance in relation to any complaint or request made, including by:

17.2.9.1 providing the Department with full details of the complaint or request;

17.2.9.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Department's instructions;

17.2.9.3 providing the Department with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Department); and

17.2.9.4 providing the Department with any information requested by the Department;

17.2.10 Permit the Department or the Department’s Representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Contractor's data processing activities (and/or those of its agents, subsidiaries and Sub-contractors) and comply with all reasonable requests or directions by the Department to enable the Department to verify and/or procure that the Contractor is in full compliance with its obligations under this Contract;

17.2.11 Provide a written description of the technical and organisational methods employed by the Contractor for processing Personal Data (within the timescales required by the Department); and

17.2.12 Not Process or otherwise transfer any Personal Data outside the European

 Economic Area. If, after the Commencement Date, the Contractor (or any

 Sub-contractor) wishes to Process and/or transfer any Personal Data

 outside the European Economic Area, the following provisions shall apply:

17.2.12.1 the Contractor shall submit a request for change to the Department which shall be dealt with in accordance with any Change Control Procedure

17.2.12.2 the Contractor shall set out in its request for change details of the following:

(a) the Personal Data which will be Processed and/or transferred outside the European Economic Area;

(b) the country or countries in which the Personal Data will be Processed and/or to which the Personal Data will be transferred outside the European Economic Area;

(c) any Sub-contractors or other third parties who will be Processing and/or transferring Personal Data outside the European Economic Area; and

(d) how the Contractor will ensure an adequate level of protection and adequate safeguards (in accordance with the Data Protection Legislation and in particular so as to ensure the Department’s compliance with the Data Protection Legislation) in respect of the Personal Data that will be Processed and/or transferred outside the European Economic Area;

17.2.12.3 in providing and evaluating the request for change, the parties shall ensure that they have regard to and comply with then-current Department, Government and Information Commissioner Office policies, procedures, guidance and codes of practice on, and any approvals processes in connection with, the Processing and/or transfers of Personal Data outside the European Economic Area and/or overseas generally; and

17.2.12.4 the Contractor shall comply with such other instructions and shall carry out such other actions as the Department may notify in writing, including:

(a) incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) in this Contract or a separate data processing agreement between the parties; and

(b) procuring that any Sub-contractor or other third party who will be Processing and/or transferring the Personal Data outside the European Economic Area enters into a direct data processing agreement with the Authority on such terms as may be required by the Department, which the Contractor acknowledges may include the incorporation of standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation).”

**17.3** The Contractor shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Department to breach any of its applicable obligations under the Data Protection Legislation.

**18 Amendment and variation**

 No amendment or variation to this Contract shall be effective unless it is in writing and signed by or on behalf of each of the parties hereto. The Contractor shall comply with any formal procedures for amending or varying contracts which the Department may have in place from time to time.

**19 Assignment and Sub-contracting**

 The benefit and burden of this Contract may not be assigned or sub-contracted in whole or in part by the Contractor without the prior written consent of the Department. Such consent may be given subject to any conditions which the Department considers necessary. The Department may withdraw its consent to any sub-contractor where it no longer has reasonable grounds to approve of the sub-contractor or the sub-contracting arrangement and where these grounds have been presented in writing to the Contractor.

**20** **The Contract (Rights of Third Parties) Act 1999**

This Contract is not intended to create any benefit, claim or rights of any kind whatsoever enforceable by any person not a party to the Contract.

**21 Waiver**

 No delay by or omission by either Party in exercising any right, power, privilege or remedy under this Contract shall operate to impair such right, power, privilege or remedy or be construed as a waiver thereof. Any single or partial exercise of any such right, power, privilege or remedy shall not preclude any other or further exercise thereof or the exercise of any other right, power, privilege or remedy.

**22 Notices**

 Any notices to be given under this Contract shall be delivered personally or sent by post or by facsimile transmission to the Contract Manager (in the case of the Department) or to the address set out in this Contract (in the case of the Contractor). Any such notice shall be deemed to be served, if delivered personally, at the time of delivery, if sent by post, 48 hours after posting or, if sent by facsimile transmission, 12 hours after proper transmission.

**23 Dispute resolution**

**23.1** The Parties shall use all reasonable endeavours to negotiate in good faith and settle amicably any dispute that arises during the continuance of this Contract.

**23.2** Any dispute not capable of resolution by the parties in accordance with the terms of Clause 23 shall be settled as far as possible by mediation in accordance with the Centre for Dispute Resolution (CEDR) Model Mediation Procedure.

**23.3** No party may commence any court proceedings/arbitration in relation to any dispute arising out of this Contract until they have attempted to settle it by mediation, but any such mediation may be terminated by either party at any time of such party wishing to commence court proceedings/arbitration.

**24 Discrimination**

**24.1** The Contractor shall not unlawfully discriminate within the meaning and scope of any law, enactment, order, or regulation relating to discrimination (whether in race, gender, religion, disability, sexual orientation or otherwise) in employment.

**24.2** The Contractor shall take all reasonable steps to secure the observance of Clause 24.1 by all servants, employees or agents of the Contractor and all suppliers and sub-contractors employed in the execution of the Contract.

**25 Law and Jurisdiction**

 This Contract shall be governed by and interpreted in accordance with English Law and the parties submit to the jurisdiction of the English courts.

 As witness the hands of the parties

Authorised to sign for and on Authorised to sign for and on

behalf of the

Secretary of behalf of Ecorys UK Private Limited Company

State for Education

Signature xxxxxxxxxxxx Signature xxxxxxxxxx

Name in CAPITALS Name in CAPITALS

Position in Organisation Position in Organisation

Director Director

Government Equalities Office

Address in full Address in full

 Albert House Quay Place -93, 92 Edward St, Birmingham B1 2RA

Sanctuary Buildings,

Great Smith Street,

London

SW1P 3BT

Date Date

28 November 2017 4th December 2017

**SCHEDULE 1**

**SPECIFICATION**

1. Introduction

The Government Equalities Office (GEO) is seeking to award a 16-month contract for the delivery of the Women’s Suffrage Centenary Grants Scheme which will run from November 2017 until the end of March 2019.

Specifically, the GEO will appoint a fund administrator to oversee the distribution of a £1.5m (incl VAT) small grants fund to individuals and organisations wishing to take part in the centenary of women’s suffrage.

The Suffrage Centenary fund, intended to inspire people throughout the country to celebrate the centenary of the beginning of women’s suffrage in 1918, was announced by the Chancellor at the Budget this year. It has an overall pot of £5m which will include spending on a small number of large events with national reach. The grant scheme is being set up to ensure that individuals and smaller groups are able to access this fund.

The grant scheme’s objectives across the three themes of the centenary - celebrate/remember, educate, participate - are to:

* Celebrate the centenary across the UK and raise awareness nationally and increase understanding of those who contributed to improving equality for women
* Educate young people about the democratic process
* Contribute to the greater involvement of women in politics.

Grants will range in size up to £125,000, however, we anticipate offering a large number of smaller grants (less than £2,000) to fund grassroots projects. The successful bidder will work at pace to manage the scheme from end to end, developing an application process, advertising the scheme, using networks to encourage grant applications from under-represented groups, assessing applications, awarding grants, agreeing key performance indicators and monitoring outputs from the funded projects, overseeing payments and evaluating outcomes from the funded projects and the fund overall.

2. Key Outcomes

a) The key outcomes for the grant scheme would be:

1. Spending at least 95% percentage of the grant scheme fund by March 2019 in line with government standards on appropriateness and value for money
2. Completing all projects, including evaluation, by March 2019
3. Reaching our target groups (such as young people, women and disengaged groups – detailed in Document 2, section 2c)
4. Finding that 50% of participants in Educate and Participate projects have increased their knowledge of women’s suffrage or democracy
5. Supporting celebration events in all regions of England
6. Contributing to the centenary fund’s overall aim that 1 in 4 people in the UK would be aware of 2018 as a key milestone for women’s right to vote.

b) To ensure that the small grants scheme has both national reach and a range of sizes from large scale “set piece” activities to local and community projects, the fund will have two dedicated streams:

* The small grants stream (up to £300k with an individual grant ceiling of £2,000) is expected to support at least 150 local or community events across England that would help deliver the “Celebrate/Remember” objective by raising national awareness of the centenary and the significance that this hard won right to vote still has today. These will be small events such as street parties celebrating local suffrage heroines.
* The larger grants stream will fund 15-30 projects (each around £2,000 to £125,000), supporting the ‘Educate’ and ‘Participate’ objectives, that increase young people’s, particularly young women’s, understanding of and engagement with democracy; and encourage women to participate in public life, covering the spectrum from grass roots and community level participation, to national parliaments. The number of projects supported is flexible so long as the administrator is meeting the requirement of providing funding to projects that cover the range. Projects could include, for example, an exhibition collecting and sharing stories of 100 local suffrage pioneers.

c) We are seeking projects that:

* Celebrate the centenary and can help support one or more of our centenary objectives Celebrate/Remember; Educate; and Participate
* Come from a range of geographic areas across England
* Engage audiences via a variety of media e.g. arts, digital, social, broadcast, classroom
* Actively seek disengaged, underrepresented and diverse audiences
* Are from a range of individuals, organisations and collaborative projects (such as regional consortia)

d) We will not fund projects that focus on:

* Campaigns
* Wholly comms-based activities.
* Research
* Activity based outside of England
* Activity promoting the cause or beliefs of a political organisation
* Activity that aims to generate profit using scheme funds (we would expect all ticketed events proceeds to be used to support the project)
* Assets (things that have a lasting value to the organisation beyond the specific project, such as phones and computers)

e) We would expect applications from charities and not for profit organisations including:

       Individuals

       Local and community groups

       HE and FE organisations

       Schools (“Celebrate” strand only)

       Cultural organisations

       Collaborative groups including regional consortia

3. Background

Since the Representation of the People Act and the Parliament (Qualification of Women) Act came into effect in 1918, women have been voting and standing in elections. Following the 2017 General Election there are now 208 women MPs (32% of the House of Commons). This is the highest number ever. However, if Parliament truly reflected the public it serves, we would expect 331 (or 51%) of all MPs to be women. The election also saw 104 constituencies across the UK without any female candidates. This left 7.5million British voters without an opportunity to vote for a woman candidate. The UK is currently 39th out of 193 countries worldwide and 12th in the European Union by the Inter-Parliamentary Union in terms of women’s political representation.

At the announcement of the Women’s Suffrage Centenary Fund earlier this year, the Chancellor outlined his aims for the fund: to give community groups a chance to celebrate the centenary and to support projects building a legacy for the future by educating young people about democracy and inspiring women to become involved in politics. This grant scheme will support community groups celebrating the centenary.

This approach supports the Minister for Women and Equalities’ priority to tackle barriers affecting women’s empowerment.

4. Statement of Requirements

The grant administrator will encourage and manage applicants for small grants to meet the agreed objectives (above) of the Centenary Fund. In defining their proposal, bidders should note that the successful bidder will be required to:

1. Show clear prior experience of success in managing grant schemes of similar size and scope, including other government contracts.
2. Set out details of prior experience and success in monitoring outputs from projects funded through similar schemes and supporting funded projects to evaluate the outcomes from their projects and activities.
3. Present a timetable showing their capacity to mobilise at pace in order to quickly evaluate applications and offer funds early in 2018, and across the centenary year. Specifically the timetable should include:
	* Dates for two bidding windows to take place by July 2018 with one opening in early January 2018.
	* Deadlines by which time bidders in each window can expect to receive a final decision.
	* Reporting and evaluation points reflecting the Management Information and KPIs outlined in the Annex (and meeting Key Outcome 2 (Document 2, Section 2a).
4. Show evidence of existing networks in the desired operational areas of women & equality, community engagement and political engagement to ensure that Key Outcome 3 (Document 2, Section 2a) is met. Alternatively this should show the ability to form/develop these networks. These networks should be used to proactively engage with leading organisations and also to facilitate active management of grants should it become clear that strong bids are not being received from a suitably wide range of organisations as laid out in Document 2, section 2c.
5. Show a comprehensive communications strategy which includes the following elements should they be required in timely fashion:
	* Advertising the scheme in a manner which aims to target diverse audiences. This should include a specific campaign targeting all MPs. Currently many MPs are receiving queries from constituents and will need clear information on how to direct interested constituents to apply for the fund.
	* Engaging in a timely and appropriate fashion with existing and potential applicants throughout the process.
	* An active communications plan for managing emerging gaps in diverse representation (geographic, etc.) as laid out in section 2c of Document 2. Whilst this may not be required, a communications plans should be in place should gaps begin to emerge.
6. Engage with existing and potential applicants throughout the process using a range of media (mail, email, telephone) ensuring that the process is inclusive and meets the needs of all audiences. Importantly this process should embed government values of equality and diversity.
7. Show a clear set of proposals for managing the grant to include:
	* Timelines for managing individual applications and payment (in line with the requirements laid out in the KPIs found in the Annex) and carrying out all relevant eligibility tests, liaising with applicants as necessary to resolve queries, supporting applicants throughout the process of obtaining any missing information and directly paying all successful applicants as payments become due.
	* Fraud prevention proposals that recognise the reputational damage to GEO/HMG that might follow funds being misspent or projects awarded funding not undertaken or completed and that are designed to mitigate these concerns. Proposals should include specific detail concerning financial due diligence checks to be run on all recipients of grants from the ‘larger grants scheme’, and recovery plans where funds are found not to be spent (we do not necessarily anticipate recovery for grants from the smaller grants stream).
	* Plans for managing the spending cap for the 2017-18 financial year of 33% of the two funds and £500,000 overall (including administrative costs and grants) and for meeting the over 95% spend required in Key Outcome 1 (Document 2, section 2a).
	* Show plans to ensure that overall the agreed bids represent diverse groups and regions as laid out in section 2c of Document 2.
	* Plans for evaluating the success of both the scheme itself and individual projects. This should include proposals to meet key outcome 4 (Document 2, section 2a) relating to increasing participant knowledge of women’s suffrage and democracy.
	* Reporting (as outlined in the Management Information provided in the Annex)
8. Show how applications would be evaluated including details of how subject matter experts would be involved, recognising the reputational damage that might be caused to GEO and HMG should funds be awarded to inappropriate organisations, and how GEO will be involved in the evaluation and decision-making on all bids over £60,000.

Subject matter expertise must cover both gender & equality and community engagement to ensure that bids are able to deliver the objectives and outcomes they propose.

1. Include information on data security specifically how any data collected in the grant application process will be managed and protected.
2. Include a funding proposal with detailed breakdown of all costs (staff, expenses etc.) for the project from start to final appraisal and how costs relate to benefits and outcomes.
3. Show how they will ensure robust value for money in delivery of the grant scheme. Where flexibilities in costs are offered, proposals should also show how this will influence value for money questions.

GEO would also:

* Retain the right to conduct spot checks of applications, evaluation and awarding process and to intervene where it felt necessary.
* Retain the right (but not duty) to attend and participate in panels/boards.
* Hold oversight of, and final decision powers on, grants over £60,000 and all larger pot proposals for ‘Celebrate’ events, regardless of quantum.
* Expect regular Management Information and meetings to discuss process, delivery and concerns
* Agree key performance indicators with the successful bidder

Our expectation on the grant process would be for:

* 33% of both funding streams to be handed over to projects by the end of March 2018
* At least 95% of both funding streams to be handed over to projects by the end of December 2018
* All projects to be completed by December 2018 with evaluation completed by March 2019
* Two application windows to take place by July 2018 with one opening in early January 2018.

5. Costs

Funds will be entirely drawn from the £5m Centenary Fund and will be paid to the grant administrator in arrears as work progresses and is monitored. The Grant Administrator is likely to require set up costs and agreed monthly administration fees.

We hope to make 160-200 awards from the two pots collectively, during the 2018 calendar year. The absolute total fund for the scheme in 2017-9, including the administration costs (the standard is 5-8% of the overall budget), VAT and grant payments, is to be £1.5m and no further funds will be available. With an absolute split of £500,000 to be spent in 2017-8 and £1m to be spent in 2018-9 (including both administration and grants).

Applicants must provide a breakdown of costs (showing VAT) under the following headings and subheadings:

Staff costs

* Non-staff delivery costs
* A breakdown of overhead costs, such as travel and subsistence, management and accommodation.
* Costs should also clearly indicate how they could vary, should the proposal have included options for management of the scheme

Applicants must also offer detail of how their bid offers best value for money by laying out:

* How costs relate directly to benefits and outcomes.
* How any proposed flexibilities/options in cost impact on value of money

6. Security of Data

Please include a security plan that explains how you will ensure that departmental and personal data will be stored securely and protected.

7. VAT

Please state clearly when submitting prices whether or not VAT will be charged.

Where the contract price agreed between the Department and contractor is inclusive of any VAT, further amounts will not be paid by the Department should a vatable supply claim be made at any later stage.

Where the overall contract price is exclusive of VAT, the Department will pay any VAT incurred at the prevailing rate (currently 20%). If the VAT rate changes the Department will pay any VAT incurred at the new rate.

It is the responsibility of tenderers to check the VAT position with HMRC before submitting a bid.

8. Proposed Procurement Timeline (this may be subject to change)

|  |  |
| --- | --- |
| Specification Published | 26th September 2017 |
| Clarification Question and Answer Period*GEO to provide answers by 10thh October 2017* | 26 September -3 October 2017 |
| Tender Response Deadline | 23th October 2017 |
| Evaluation | 23-30th October 2017 |
| Potential Clarification Meetings with shortlisted organisations (if necessary) | 26th October 2017 |
| HMG Approvals | 30th October- 3 November 2017 |
| Suppliers Notified of Outcome | 3 November 2017 |
| 10 day hold | 3 - 13th November 2017 |
| Contract Awarded | 16th November 2017 |

9. Evaluation Criteria

The award criteria are set out below (further details in Annexes A & B).

* Quality: (70%)
* Experience
* Subject Matter Expertise
* Timetable
* Networks
* Communication Strategy
* Grant Management
* Data Security
* Price: (30%)
* Cost
* Value for Money

10. Other issues

The GEO reserves the right to:

* Withdraw this tender at any time without awarding a call-off contract
* Make whatever changes it sees fit to the procurement timeline.

Any communications and marketing plans promoting the scheme would be subject to clearance by GEO’s communications team. For plans that include paid-for marketing activities, please allow three weeks for sign off. Marketing plans should follow the “OASIS” structure, which is the standard model used for developing government communications plans. More information about OASIS and templates can be found on the Government Communications Service website. In particular, you will need to demonstrate use of insight to inform the proposed communications approach as well as clear objectives and a defined target audience. You will also need to outline how you will monitor and evaluate your plan.

As a member of a public body, the GEO is subject to the provisions of the Freedom of Information Act 2000 (FOIA) in respect of information it holds (including third party information). Any member of the public or other interested party may make a request for information.

The Authority shall treat all Suppliers’ responses as confidential during the procurement process. Requests for information received following the procurement process shall be considered on a case-by-case basis, applying the principles of FOIA, which permits certain information to be withheld, for example where disclosure would be prejudicial to a party’s commercial interests, and in accordance with the GEO’s transparency obligations.

Suppliers are therefore responsible for ensuring that any confidential or commercially sensitive information, the disclosure of which would be likely to have a negative effect on the supplier, has been clearly identified to GEO when submitting a tender. The GEO shall consider any requests from a supplier that certain information should remain confidential but shall make the final decision as to whether any such information should be disclosed pursuant to the FOIA.

11. Application process

The grant scheme has two pots, one for small local or community events to celebrate the centenary and one for larger projects helping to deliver our policy objectives. We would expect the proposed application process is proportionate in managing financial risk and evaluation for those pots. In particular, we would expect that, for grants for under £2,000, there should be a light touch process in application, assessment and evaluation. See attached annex F for a suggested process.

**SCHEDULE 2**

**Ecorys original bid to GEO- attached separately due to document size.**

**SCHEDULE 3**

**SGF Set up timetable**

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Date** | **GEO Action required** | **Owner** **(to be allocated/ reviewed on weekly calls)** |
| GEO to confirm chosen option for stand up | Friday 17th November | To confirm approach | GEO |
| Contract/letter of comfort issued | Monday 20th November | GEO to issue | GEO |
| Ecorys to draft application form and eligibility criteria for Wave 1 | Thursday 23rd November | Comments back on application form and eligibility by **9am****Monday 27th November** | Ecorys |
| Application form and eligibility criteria finalised (off line)  | Tuesday 28th November  | Sign off by 5pm | GEO |
| Handover of application form to Flexigrant for build of on line form | To commence Wednesday 29th November |  | Ecorys |
| V1 FAQ’s and Guidance drafted by Ecorys | Friday 1st December | Comments by **Weds 6th December** | Ecorys |
| V1 comms plan (for launch stage) drafted | Friday 1st December | Sign off by **Tuesday 5th** | Ecorys |
| GEO messaging and handling agreed for: if too much demand, dealing with rejections etc.  | 4th December |  | GEO |
| [www.womensuffragecentenaryfund.com](http://www.womensuffragecentenaryfund.com) (title tbc)Simple Page designed and built by Ecorys as “launch pad” into on line form. To include guidance, FAQs etc. and route to LGF in timeEcorys to host | Prepared by 4th December  | **GEO sign off of web page by 5th December** | Ecorys |
| Grant guidance and FAQs completed | Monday 4th December  | **Sign off by Tuesday 5th Dec** | Ecorys |
| Ecorys project email address set upAddress tbc | Wednesday 6th December |  | Ecorys |
| Gov.uk web page prepared with basic info and link to Ecorys grants sitelink tbc  | 7th December | To lead and oversee and provide copy  | GEO |
| Ecorys Web page goes live with “coming soon” banner or similar | Thursday 7th December  | **GEO To announce this (recommend low key)** | Ecorys |
| Answering potential applicant queries | From 7th December – 22nd DecemberFrom 4th January – 31st January |  | Ecorys |
| V1 on line application form ready for testing & feedback | Monday 11th December |  | Fluent Technology |
| Guidance etc. uploaded and built into on line application form where required | 15th December |  | Ecorys/ Fluent |
| V2 of application form ready  | 19th December |  | Fluent |
| R1 Testing of application form and process | 20th December |  | Ecorys |
| Feedback of R1 testing | 22nd December |  | Ecorys |
| Auto reply email- can direct people to FAQs and say back on 3rd Jan | 22nd Dec to 3rd Jan |  | Ecorys |
| R2 Testing of application form and process | 2nd January |  | Ecorys |
| Feedback of R2 testing & finalising  | 2nd- 5th January |  | Ecorys/Fluent |
| Round 1 of WS Small Grants Fund opens for online applications | 4th January | Announcements as per agreed comms plan | All |
| Tweets and Social Media posts announcing opening | 4th January | **Liaison GEO comms and Ecorys/ sign off of posts** | Ecorys/GEO |
| Live monitoring of application portal site | From 4th January |  | Ecorys/ Fluent |
| Ongoing review of first wave applications and recommendation to GEO  | From 4th January |  | Ecorys |
| GEO Sign off of first batch of grants | From 5th January |  | GEO |
| Wave 1 Applicants notified of approval/rejection  | From Wednesday 10th Jan |  | Ecorys |
| Wave 1 payments made | From Friday 19th January |  | Ecorys |
| Closing of first wave of small grants window | Friday 31st January |  | Ecorys |
| Review and scheduling of next wave and targeting, refined messaging etc.  | By Friday 2nd February |  | All |

**SCHEDULE 4 – MILESTONE AND PAYMENT PLAN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Dec-17** | **Jan-18** | **Feb-18** | **March** | **April** | **May-18** | **Jun-18** | **Jul-18** | **Aug-18** | **Sep-18** | **Oct-18** | **Nov-18** | **Dec-18** | **Total** |
| **2018** | **2018** |
| **Small Grants Fund** | Design and build |   | review |   | SGF Round 2 open | SGF round 2 close |   |  | SGF Round 3 open | SGF round 3 closes |   |   |   |  |
|   |   |   |   |  |   |   |
| Round 1 Soft launch 7 December | SGF on line launch 4th January |   | Budget review |   |   |   |
| **Small Grant Funds committed (inc. VAT)** |   | £120,000 |   |   |   | £120,000 |   |   |   | £60,000 |   |   |   | **£300,000** |
| **Large Grants Fund** | Design and Build | Launch | LGF Call 1 closes |   | LGF Call 2 open | LGF closes |   |  |   |   |   |   |   |  |
| LGF Call 1 open by 31 Jan (tbc) |   |   |   |   |
|   | Grants Panel |   |   |   |
|   |   | Grants panel |   |   |
| **Large Grant Funds committed (inc. VAT)** |   |   | £340,000 |   |   | £752,000 |   |   |   |   |   |   |   | **£1,092,000** |
| **Administration Fee inc. VAT** | £10,000 | £10,000 | £10,000 | £10,000 | £9,000 | £9,000 | £9,000 | £9,000 | £8,000 | £8,000 | £8,000 | £4,000 | £4,000 | **£108,000** |
| **Total Budget (inc. VAT) paid out (Cumulative)** | 10000 | 140000 | 490000 | £500,000 | £509,000 | £638,000 | £647,000 | £1,408,000 | £1,416,000 | £1,484,000 | £1,492,000 | £1,496,000 | £1,500,000 | **£1,500,000** |
|

\*\*\*''the above prices are inclusive of VAT\*\*\*

**2** Funds allocated to a particular expenditure heading in the table at paragraph 1 ("the Table") are available for that expenditure heading only. Funds allocated to a particular accounting year are available for that accounting year only. The allocation of funds in the Table may not be altered except with the prior written consent of the Department.

**3** The Contractor shall maintain full and accurate accounts for the Service against the expenditure headings in the Table. Such accounts shall be retained for at least 6 years after the end of the financial year in which the last payment was made under this Contract. Input and output VAT shall be included as separate items in such accounts.

**4** The Contractor shall permit duly authorised staff or agents of the Department or the National Audit Office to examine the accounts at any reasonable time and shall furnish oral or written explanations of the account if required. The Department reserves the right to have such staff or agents carry out examinations into the economy, efficiency and effectiveness with which the Contractor has used the Department's resources in the performance of this Contract.

**4.1** The Contractor shall also permit persons duly authorised by the European Court of Auditors and the European Commission to examine the accounts at any reasonable time and shall furnish oral or written explanation of the accounts if required.

**5** Invoices shall be prepared by the Contractor \*\*\**either state a period of time (e.g. monthly) or insert the term* 'on the invoice dates specified in the Table' \*\*\* in arrears and shall be detailed against the expenditure headings set out in the Table. The Contractor or his or her nominated representative or accountant shall certify on the invoice that the amounts claimed were expended wholly and necessarily by the Contractor on the Service in accordance with the Contract and that the invoice does not include any costs being claimed from any other body or individual or from the Department within the terms of another contract.

**6** Invoices shall be sent, within *30 days* of the end of the relevant month in accordance with SCHEDULE 4 (MILESTONE AND PAYMENT PLAN) to SSCL Accounts Payable Team, Room 6124, Tomlinson House, Norcross, Blackpool FY5 3TA, quoting the Contract reference number. The Department undertakes to pay correctly submitted invoices within 5 days of receipt. The Department is obliged to pay invoices within 30 days of receipt from the day of physical or electronic arrival at the nominated address of the Department. Any correctly submitted invoices that are not paid within 30 days will be subject to the provisions of the Late Payment of Commercial Debt (Interest) Act 1998. A correct invoice is one that: is delivered in timing in accordance with the contract; is for the correct sum; in respect of goods/services supplied or delivered to the required quality (or are expected to be at the required quality); includes the date, supplier name, contact details and bank details; quotes the relevant purchase order/contract reference and has been delivered to the nominated address. If any problems arise, contact the Department's Contract Manager. The Department aims to reply to complaints within 10 working days. The Department shall not be responsible for any delay in payment caused by incomplete or illegible invoices.

**7** The Contractor shall have regard to the need for economy in all expenditure. Where any expenditure in an invoice, in the Department's reasonable opinion, is excessive having due regard to the purpose for which it was incurred, the Department shall only be liable to reimburse so much (if any) of the expenditure disallowed as, in the Department's reasonable opinion after consultation with the Contractor, would reasonably have been required for that purpose.

**8** If this Contract is terminated by the Department due to the Contractors insolvency or default at any time before completion of the Service, the Department shall only be liable under paragraph 1 to reimburse eligible payments made by, or due to, the Contractor before the date of termination.

**9** On completion of the Service or on termination of this Contract, the Contractor shall promptly draw-up a final invoice, which shall cover all outstanding expenditure incurred for the Service. The final invoice shall be submitted not later than 30 days after the date of completion of the Service.

**10** The Department shall not be obliged to pay the final invoice until the Contractor has carried out all the elements of the Service specified as in Schedule 1.

**11** It shall be the responsibility of the Contractor to ensure that the final invoice covers all outstanding expenditure for which reimbursement may be claimed. Provided that all previous invoices have been duly paid, on due payment of the final invoice by the Department all amounts due to be reimbursed under this Contract shall be deemed to have been paid and the Department shall have no further liability to make reimbursement of any kind.

**SCHEDULE 5**

**Departmental Security Standards**

1. **Departmental Security Standards for Business Services and ICT Contracts**

|  |  |
| --- | --- |
| “BPSS”“Baseline Personnel Security Standard” | a level of security clearance described as pre-employment checks in the National Vetting Policy. |
| “CCSC”“Certified Cyber Security Consultancy” | is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website:<https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy>  |
| “CCP”“Certified Professional” | is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. See website:<https://www.ncsc.gov.uk/scheme/certified-professional>  |
| “CC”“Common Criteria” | the Common Criteria scheme provides assurance that a developer’s claims about the security features of their product are valid and have been independently tested against recognised criteria.  |
| “CPA”“Commercial Product Assurance”[formerly called “CESG Product Assurance”] | is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. See website: <https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>  |
| “Cyber Essentials”“Cyber Essentials Plus” | Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. |
| “Data”“Data Controller”“Data Processor”“Personal Data”“Sensitive Personal Data” “Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Act 1998 |
| "Department’s Data"“Department’s Information” | is any data or information owned or retained in order to meet departmental business objectives and tasks, including:(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:(i) supplied to the Contractor by or on behalf of the Department; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or(b) any Personal Data for which the Department is the Data Controller; |
| “DfE”“Department” | means the Department for Education |
| “Departmental Security Standards” | means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver. |
| “Digital Marketplace / GCloud” | the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework. |
| “FIPS 140-2” | this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled ‘Security Requirements for Cryptographic Modules’. This document is the de facto security standard used for the accreditation of cryptographic modules. |
| “Good Industry Practice”“Industry Good Practice” | means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “Good Industry Standard”“Industry Good Standard” | means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “GSC”“GSCP” | means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications |
| “HMG” | means Her Majesty’s Government |
| “ICT” | means Information and communications technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution |
| “ISO/IEC 27001” “ISO 27001” | is the International Standard for Information Security Management Systems Requirements |
| “ISO/IEC 27002” “ISO 27002” | is the International Standard describing the Code of Practice for Information Security Controls. |
| “ISO 22301” | is the International Standard describing for Business Continuity |
| “IT Security Health Check”“Penetration Testing” | means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system. |
| “Need-to-Know” | the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties. |
| “NCSC” | The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. This supersedes CESG, which was formerly the National Technical Authority. The NCSC website is <https://www.ncsc.gov.uk>  |
| “NCSC IAP” “NCSC Information Assurance Policy Portfolio”[Formerly called “CESG IAP”] | means the NCSC (formerly CESG) Information Assurance policy Portfolio containing HMG policy and guidance on the application of ‘security assurance’ for HMG systems. |
| “OFFICIAL”“OFFICIAL-SENSITIVE”  | the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services. the ‘OFFICIAL–SENSITIVE’ caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy. |
| “Secure Sanitisation” | Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable. Secure sanitisation was previously covered by “Information Assurance Standard No. 5 - Secure Sanitisation” (“IS5”) issued by the former CESG. Guidance can now be found at: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>  |
| “Security and Information Risk Advisor” “CCP SIRA”“SIRA” | the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also:<https://www.ncsc.gov.uk/articles/about-certified-professional-scheme>  |
| “SPF”“HMG Security Policy Framework” | This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. |
| ” Tailored Assurance”[formerly called “CTAS”, or,” CESG Tailored Assurance”] | is an ‘information assurance scheme’ which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. |

* 1. The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
* *(Guidance: Providers on the HMG Digital Marketplace / GCloud or Public Service Network (PSN) that have demonstrated compliance, as part of their scheme application, to the relevant scheme’s security framework, such as the HMG Cloud Security Principles for the HMG Digital Marketplace / GCloud, may on presentation of suitable evidence of compliance be excused from compliance to similar clauses within the DfE Security Clauses detailed in this section (Section 12).)*
	1. Where the Contractor will provide ICT products or Services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - [Action Note 09/14](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme”. The certification scope must be relevant to the services supplied to, or on behalf of, the Department.
* *(Guidance: The Department’s expectation is that the certification scope will be relevant to the services supplied to, or on behalf of, the Department. However, where a contractor or (sub) contractor is able to evidence a valid exception or certification to an equivalent recognised scheme or standard, such as ISO 27001, then certification under the Cyber Essentials scheme could be waived and this clause may be removed. Changes to the Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14 25 May 2016 will be tracked by the DSU)*
* *(Guidance: The terms OFFICIAL and OFFICIAL-SENSITIVE are taken from the Government Security Classification Policy (GSCP). The Department’s expectations are that all contractors shall handle the Department’s information in a manner compliant with the GSCP – see 12.4 below. Details of the GSCP can be found on the GOV.UK website at:* [*https://www.gov.uk/government/publications/government-security-classifications*](https://www.gov.uk/government/publications/government-security-classifications)*.)*

 *[Use the appropriate Clause 12.3]*

* 1. [Either]

The Contractor shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

*(Guidance: The Department’s expectation is that suppliers demonstrating conformance to ISO/IEC 27001 will be able to provide the Department with copies of their Scope of Conformance and Statement of Applicability.)*

[Or, for contracts involving the processing of particularly sensitive data]

12.3 The Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

* *(Guidance: The Department’s expectation is that suppliers claiming certification to ISO/IEC 27001 shall provide the Department with copies of their Scope of Certification, Statement of Applicability and a valid ISO/IEC 27001 Certificate issued by an authorised certification body. Where the provider is an SME that has a valid Cyber Essentials certification then certification under the ISO/IEC 27001 scheme could be waived and this clause may be removed.)*
	1. The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
* *(Guidance: The Department’s expectations are that all contractors shall handle the Department’s information in a manner compliant with the GSCP. Details of the GSCP can be found on the GOV.UK website at:* [*https://www.gov.uk/government/publications/government-security-classifications*](https://www.gov.uk/government/publications/government-security-classifications)*.)*
	1. Departmental Data being handled in the course of providing the ICT solution or service must be segregated from other data on the Contractor’s or sub-contractor’s own IT equipment to both protect the Departmental Data and enable it to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Contractor and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 12.14.
* *(Guidance: Advice on HMG secure sanitisation policy and approved methods are described at* [*https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media*](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)*)*
	1. The Contractor shall have in place and maintain physical security and entry control mechanisms (e.g. door access) to premises and sensitive areas and separate logical access controls (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.
* *(Guidance: Where the contractor’s and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause and it need not be included.)*
	1. The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.
* *(Guidance: Where the contractor’s and sub-contractor services are wholly carried out using Departmental ICT resources or locations managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause and it need not be included.)*
	1. Any electronic transfer methods across public space or cyberspace, including third party provider networks must be protected via encryption which has been certified to a minimum of FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.
* *(Guidance: The terms “public space” and “cyberspace” are used to describe the internet and any commercially provided third party network used to transmit Departmental information. Even where the contractor’s and sub-contractor services are wholly carried out using Departmental ICT resources managed directly by the Department as part of the service, if there is still the possibility of emails being sent to external addresses, this clause should be included.)*
	1. Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 12.10 and 12.11 below.
	2. Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to the Department.
* *(Guidance: Where the use of removable media as described at Clause 12.9 above is either prohibited or not required in order to deliver the service this clause shall be revised as follows: - ‘The use of removable media in any form is not permitted’.)*
	1. All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to a minimum of FIPS140-2 standard or use another encryption standard that is acceptable to the Department.
* *(Guidance: Where there is no suitable FIPS140-2 encryption product available to provide the necessary full-disk encryption, the Department shall agree a suitable alternative product that meets ‘industry good practice’ in this area with the contractor or sub-contractor. Where the contractor’s and sub-contractor services are wholly carried out using Departmental ICT resources managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause and it need not be included.)*
	1. Whilst in the Contractor’s care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure waste paper organisation.
* *(Guidance: The term ‘lock and key’ is defined as: “securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user’s sole control and to which they hold the keys”.)*
	1. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.
* *(Guidance: The term ‘under cover’ means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when travelling outside of official premises or buildings).*
	1. At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Contractor’s ICT infrastructure must be securely sanitised or destroyed in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Contractor or sub-contractor shall protect the Department’s information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.
* *(Guidance: Where no departmental information or data shall be held by the Contractor or sub-contractor, in either physical or logical form this clause may be removed.)*
* *(Guidance: Where there is no acceptable secure sanitisation method available for a piece of equipment, or it is not possible to sanitise the equipment due to an irrecoverable technical defect, the storage media involved shall be destroyed using an HMG approved method described at* [*https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media*](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)*.)*
	1. Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” and the appropriate level of security clearance, as required by the Department for those individuals whose access is essential for the purpose of their duties. All employees with direct or indirect access to Departmental Data must be subject to pre-employment checks equivalent to or higher than the HMG Baseline Personnel Security Standard (BPSS)
* *(Guidance: Further details of the requirements for HMG BPSS clearance are available on the website at:* [*https://www.gov.uk/government/publications/government-baseline-personnel-security-standard*](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard))
	1. All Contractor or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.
	2. The Contractor shall, as a minimum, have in place robust and ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might be, or could lead to, a disruption, loss, emergency or crisis. When a certificate is not available it shall be necessary to verify the ongoing effectiveness of the ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures, to the extent that the Contractor must have tested/exercised these plans within the last 12 months and produced a written report of the test/exercise, outcome and feedback, including required actions.
* *(Guidance: The creation of robust business continuity and disaster recovery plans are aligned with industry good practice and it is the Department’s expectation that all vendors providing services or infrastructure to the Department will have plans that are aligned to the ISO 22301 standard in place. Further information on the requirements of ISO 22301 may be found in the standard.)*
	1. Any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution, or any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, shall be investigated immediately and escalated to the Department by a method agreed by both parties.
* *(Guidance: The Department’s expectation is that non-compliances, or any suspected or actual breach of the confidentiality, integrity or availability of the Department’s Data shall be reported as incidents and investigated by the vendor with outcomes being notified to the Department.)*
	1. The Contractor shall ensure that any IT systems and hosting environments that are used to hold Departmental Data being handled, stored or processed in the course of providing this service shall be subject to an independent IT Health Check (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
* *(Guidance: Further information on IT Health Checks and the NCSC CHECK Scheme which enables penetration testing by NCSC approved companies can be found on the NCSC website at:* [*https://www.ncsc.gov.uk/scheme/penetration-testing*](https://www.ncsc.gov.uk/scheme/penetration-testing)*.)*
	1. The Contractor or sub-contractors providing the service will provide the Department with full details of any actual storage outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management or support function from outside the UK. The Contractor or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department.
* *(Guidance: The offshoring of HMG information outside of the UK is subject to approval by the Departmental SIRO and, in some cases, also by the Office of the Government Senior Information Risk Owner (OGSIRO). Further information on this process can be found at:* [*https://ogsirooffshoring.zendesk.com/hc/en-us/articles/203107991-HMG-s-Offshoring-Policy*](https://ogsirooffshoring.zendesk.com/hc/en-us/articles/203107991-HMG-s-Offshoring-Policy))
	1. The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor’s, and any sub-contractors, compliance with the clauses contained in this Section.
	2. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.