CONTRACT FOR STEP UP TO SOCIAL WORK COHORT 7 SUPPORT CONTRACTOR

This contract is made on the 18 day of January 2021

1 THE SECRETARY OF STATE FOR EDUCATION of Sanctuary Buildings, 20 Great Smith Street, London, SW1P 3BT ("**DFE**"); and

2 CAPITA BUSINESS SERVICES LIMITED (registered company number 02299747 whose registered office is at 65 Gresham Street, London EC2V 7NQ ("the Contractor")

each a "**Party**" and together the "**Parties**".

It is agreed that:

1. this contract, together with the attached schedules and annexes, collectively form the "**Contract**"; and

2. if there is a conflict between the provisions of the clauses of the Contract and the provisions of the schedules, the following order of precedence shall apply:

(a) (Terms and Conditions);
(b) schedule 1 (Specification);
(c) schedules 2 to 8; and
(d) schedule 9 (Contractor's Solution).

The Contract has been executed on the date stated at the beginning of this page.

Terms and Conditions

CONTENTS

CLAUSE

Recitals

The Contractor has agreed to deliver a fully managed service for the Step Up programme on the terms and conditions set out in this Contract.

1 Definitions and Interpretation

1.1 In this Contract the following words shall mean:-

"the Services""	the services to be performed by the Contractor as described in Schedule 1;
"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"	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;
“Commercially Sensitive Information”	The information set out at Schedule 9 which the Contractor has indicated to the Department that, if disclosed by the Department, would cause the Contractor significant commercial disadvantage or material financial loss
“the Contract Manager”	Individual named by the Department to represent and communicate their interests. Any changes to this individuals name or contact details will be communicated to the Contractor as soon as is practical.
“Contract Period”	The start and end date of the contract as set out in Clause 2 subject to any extensions.
"Contractor Personnel"	all employees, agents, and contractors of the Contractor and/or of any Sub-contractor;
“Contractor’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 Contractor, 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;
“the Contractors Contract Manager	Individual named by the Contractor to represent and communicate their interests. Any changes to this individuals name or contact details will be communicated to the Department as soon as is practical;
“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;

“Contracts Finder”	the Government’s publishing portal for public sector procurement opportunities;
"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;
“Controller”, “Joint Controller”, “Processor,” “Data Subject”, “Personal Data”, “Personal Data Breach”, “Data Protection Officer”	take the meaning given in the GDPR;
“Crown”	means Queen Elizabeth II and any successor;
"Crown Body"	any department, office or agency of the Crown;
“Data Loss Event”	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“DPA 2018”	Data Protection Act 2018;
“Data Protection Impact Assessment”	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
“Data Protection Legislation”	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;
“Data Subject Request”	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Department’s Confidential	all Personal Data and any information, however it

Information"	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;
"Department's Intellectual Property Rights"	means all Intellectual Property Rights that arise, are created or developed by the Contractor exclusively for the Department as part of, or in connection with the performance of the Services, including Intellectual Property Rights subsisting in any process, deliverables, documents or works;
"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;
“GDPR”	the General Data Protection Regulation (Regulation (EU) 2015/579);
“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;
"Intellectual Property Rights"	means any copyright, rights in designs, database rights, domain names, trade marks, service marks, patents or any applications for any of the foregoing, know-how or similar rights or obligations (whether registerable or not) including Moral Rights as defined in Chapter IV of the

	Copyright, Designs and Patents Act 1988;
“Joint Controllers”	Where two or more Controllers jointly determine the purposes and means of processing;
“Key Personnel”, “Key Sub-Contractors”	means any of the Personnel or Sub-Contractors identified as such in schedule 7;
“Law”	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;
“LED”	Law Enforcement Directive (Directive (EU) 2015/580)
“Processor Personnel”	employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract;
“Property”	means the property, other than real property, issued or made available to the Contractor by the Client in connection with the Contract;
“Protective Measures”	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those set out in 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 2003/351/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;
"Sub-processor"	any third Party appointed to process Personal Data on behalf of the Contractor related to this Contract;
"VCSE"	means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"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 and the neuter. References to a person include any individual, firm, unincorporated association or body corporate.

2 Commencement and Continuation

2.1 The Contractor shall commence the Services on the Effective Date and, subject to any provision of this Contract for earlier termination, or extension set out in this clause 2, will terminate at the end of the Initial Term.

2.2 DFE may extend the Initial Term for such further period as the DFE may choose by giving not less than 3 months' written notice to the Contractor prior to the expiry of the Initial Term.

3 Contractor's Obligations

3.1 The Contractor shall provide the Services in the Area in accordance with the Specification and undertake and be responsible for all obligations of the Contractor in respect of the Services.

3.2 The Contractor shall comply with the accounting and information provisions.

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 2 provided that the Department has received full and accurate information and documentation as required by Schedule 2 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 in writing of any material change to the Department's requirement under this Contract as described in Schedule 6 of this Contract.

5.2 The Contractor shall use commercially reasonable 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, and where supported by evidence, 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 give to the Department if so requested a list of all persons who are or may be at any time directly concerned with the performance of this Contract specifying the capacity in which they are concerned with the provision of the Services and giving such other particulars as the Department may reasonably require.

7.5 If the Department notifies the Contractor that it considers that an employee or sub-contractor is not appropriately qualified or trained to provide the Services or otherwise is not providing the Services in accordance with this Contract, then the Contractor shall, as soon as is reasonably practicable, take all such steps as the Department considers necessary to remedy the situation or, if so required by the Department, shall remove the said employee or sub-contractor from providing the Services and shall provide a suitable replacement (at no cost to the Department).

7.5 The Contractor shall take all reasonable steps to avoid changes of employees or sub-contractors assigned to and accepted to provide the Services under the Contract except whenever changes are unavoidable or of a temporary nature. The Contractor shall give at least one month's written notice to the Contract Manager of proposals to change Key Personnel or Key Sub-Contractors.

7.7 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.

7.8 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.

7.9 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 Intellectual Property Rights

8.1 It is acknowledged and agreed between the parties that all existing or future Department's Intellectual Property Rights shall vest in the Crown absolutely.

8.2 Any Intellectual Property Rights of the Contractor which are in existence at the date of this Contract and which are comprised in or necessary for or arising from the performance of the Services owned by the Contractor ("**Background Intellectual Property**") shall remain in the ownership of the Contractor but in consideration of the fees payable pursuant to this Contract, the Contractor hereby grants to the Department in respect of such Background Intellectual Property an irrevocable, non-exclusive, royalty-free, licence for the duration of the Contract with rights to grant sub-licences.

8.3 The Contractor agrees that at the request and cost of the Department it will and procure that its officers, employees and agents will at all times do all such reasonable acts and execute all such documents as may be reasonably necessary or desirable to ensure that the Department receives the full benefit of all of its rights under this Contract in respect of the Department's Intellectual Property Rights or to assist in the resolution of any question concerning the Intellectual Property Rights.

8.4 The Contractor hereby waives any Moral Rights as defined at Chapter IV of the Copyright, Designs and Patents Act 1988.

8.5 The Contractor warrants:

8.5.1 that the Department's Intellectual Property Rights comprise the original work of and were created by or on behalf of the Contractor or are otherwise licensed to the Contractor on a basis which is compatible with the rights granted in clause 8.2 above;

8.5.2 that the Department's Intellectual Property Rights have not and will not be copied wholly or in part from any other work or material;

8.5.3 that the use of or exercise by the Department of the Department's Intellectual Property Rights and the Background Intellectual Property will not infringe the rights of any third party;

8.5.4 that the Contractor has not granted or assigned any rights of any nature in the Department's Intellectual Property Rights to any third party.

8.5 The Contractor shall ensure that any Department copyright materials reproduced by or on behalf of the Contractor under the delivery of this contract shall be marked with the following copyright notice " © Crown Copyright ***year of publication***".

9 Warranty, Indemnity and Limit of Liability

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 where the Contractor has failed to comply with Clause 9.2.1, and provided there is not a bona fide dispute which has been raised in accordance with Clause 23 (Dispute resolution), deduct sums due to the Contractor for the period such failure continues equivalent to:

9.2.2.1 any additional operational and/or administrative costs and expenses incurred by the DFE, including costs relating to time spent by or on behalf of the DFE in dealing with the consequences of the default;

9.2.2.2 any additional operational and/or administrative costs and expenses incurred by the DFE, including costs relating to time spent by or on behalf of the DFE in dealing with the consequences of the default;

9.2.2.3 any wasted expenditure or charges;

9.2.2.4 the additional costs of procuring a Replacement Contractor for the remainder of the Contract and or replacement deliverables;

9.2.2.5 any compensation or interest paid to a third party by the DFE; and

9.2.2.6 any fine or penalty incurred by the DFE and any costs incurred by the DFE in defending any proceedings which result in such a fine or penalty.

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 Subject always to the limitations on its liability in Clause 9.8, 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.

9.5 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 documentary evidence that the policy or policies are properly maintained.

9.6 The limits on liability under Clauses 9.7 (Exclusion of Liability) and 9.8 (Limitations on Liability) shall not apply to:

9.6.1 death or personal injury caused by negligence;

9.6.2 fraud or fraudulent misrepresentation;

9.6.3 Department's liability to pay the Charges and other sums due to the Contractor;

9.6.4 any obligations of a party pursuant to Clause **Error! Reference source not found.** (Confidentiality);

9.6.5 the Contractor's warranty at Clause 8.5.3; or

9.6.6 any other matter for which it would be unlawful to exclude or attempt to exclude its liability.

9.7 **Exclusion of Liability**. Neither party shall be liable to the other for any:

9.7.1 indirect, special or consequential Losses arising in connection with this Contract;

9.7.2 loss of profits, loss of sales, anticipated savings or goodwill, loss of business opportunity or contracts in each case whether direct or indirect

even if such losses could have been foreseen.

9.8 **Limitations on Liability.** Subject to Clauses 9.6 (Unlimited Liability) and 9.7 (Exclusion of Liability), the total aggregate liability of each party for all other losses, whether arising from tort (including negligence), indemnity, breach of contract or otherwise

9.8.1 in respect of damage to property is limited in respect of any one incident or series of connected incidents; and

9.8.2 in respect of any claim not covered by clause 9.8.1, is limited in each calendar year in aggregate to percentage of the sum of the Charges payable in that year.

9.9 Without prejudice to its other rights or remedies, any delay or non-performance by Contractor of its obligations under this Contract will be excused to the extent it is caused by acts or omissions of the Department, its consultants or subcontractors.

9.10 The parties shall each be subject to a general duty to mitigate their losses.

10 Termination

10.1 This Contract may be terminated by either party giving to the other party at least 30 days' 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 and not less than 30 days. 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 an irremediable 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 (save in the case of a solvent amalgamation or reconstruction); 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 1985;

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;

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 its 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 its 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 Clause 12 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 Services 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 12.5.1 (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

12.6.5 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 shall consult with the Contractor to inform its decision regarding any redactions to remove Commercially Sensitive Information 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 consult with the Contractor to inform its decision regarding any redactions to remove Commercially Sensitive Information, but 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 Services:

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.

13.5 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 in accordance with clause 14 (Access and Information).

14 Access and Information

The Contractor shall provide access at all reasonable times and on reasonable notice 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. The Department shall so far as possible limit the number and frequency of audits it carries out in any calendar year during the term of this contract to avoid disruption to the Contractor.

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 up to 6 months 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 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.

16.2 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.

16.3 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.

16.4 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

17.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Department is the Controller and the Contractor is the Processor unless otherwise specified in Schedule 3a. The only processing that the Processor is authorised to do is listed in Schedule 3a by the Controller and may not be determined by the Processor.

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

17.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

17.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;
17.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;
17.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and
17.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

17.4.1 process that Personal Data only in accordance with Schedule 3a, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

17.4.2 ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

17.4.3 ensure that :

(i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 3a);
(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(a) are aware of and comply with the Processor's duties under this clause;
(b) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
(c) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and
(d) have undergone adequate training in the use, care,

protection and handling of Personal Data; and

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 45 or LED Article 37) as determined by the Controller;
(ii) the Data Subject has enforceable rights and effective legal remedies;
(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

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

17.5 Subject to clause 17.5, the Processor shall notify the Controller promptly if it:

17.5.1 receives a Data Subject Request (or purported Data Subject Request);
17.5.2 receives a request to rectify, block or erase any Personal Data;
17.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
17.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
17.5.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
17.5.6 becomes aware of a Data Loss Event.

17.6 The Processor's obligation to notify under clause 17.5 shall include the provision of further information to the Controller in phases, as details become available.

17.7 Taking into account the nature of the processing, the Processor shall provide the Controller with all reasonable assistance in relation to either Party's obligations under Data Protection Legislation insofar as they relate to this Contract and any complaint, communication or request made under clause 17.5 (and insofar as possible within the timescales reasonably required by the

Controller) including by promptly providing:

17.7.1 the Controller with full details and copies of the complaint, communication or request;
17.7.2 such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
17.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
17.7.4 assistance as requested by the Controller following any Data Loss Event;
17.7.5 assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

17.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

17.8.1 the Controller determines that the processing is not occasional;
17.8.2 the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
17.8.3 the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

17.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

17.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:

17.11.1 notify the Controller in writing of the intended Sub-processor and processing;
17.11.2 obtain the written consent of the Controller;
17.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 17 such that they apply to the Sub-processor; and
17.11.4 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

17.12 The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

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

17.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

17.15 Where the Parties include two or more Joint Controllers as identified in Schedule 3a in accordance with GDPR Article 25, those Parties shall enter into a Joint Controller agreement based on the terms outlined in Schedule 3b in replacement of Clauses 17.1-17.14 for the Personal Data under Joint Control.

18 Amendment and variation

The parties shall comply with the requirements of Schedule 6 (Change Control Procedure).

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 either party without the prior written consent of the other. In the case of a request by the Contractor, 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

22.1 Any notice, demand or communication in connection with the Contract shall be in writing and may be delivered by hand, pre-paid first class post or (where being sent to an address in a different country to where posted) airmail, or e-mail, addressed to the recipient at its registered office or its address (or such other address, or e-mail address as may be notified in writing from time to time).

22.2 The notice, demand or communication shall be deemed to have been duly served:

22.2.1 if delivered by hand, when left at the proper address for service;

22.2.2 if given or made by prepaid first class post 48 hours after being posted or in the case of airmail 14 days after being posted;

22.2.3 if made by e-mail, at the time of transmission, dispatched as a pdf attachment to an e-mail to the correct e-mail address without any error message or, in the case of transmission by e-mail where the time of transmission is not between 9.00 am and 5.00 pm, service shall be deemed to occur at 9.00 am on the next following Business Day (such times being local time at the address of the recipient).

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

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

Schedule 1

The Specification

1. Business Requirements

1.1 Introduction and Scope

The purpose of this document is to specify the requirements to deliver a fully managed service for the Step Up programme. The scope of this document is limited to the requirements for the Invitation to Tender (ITT).

1.2 Background and Context

Step Up to Social Work complements our reform programme and our commitment to raising the quality of social work practice, with a particular focus on the practice of child and family social workers undertaking statutory social work.

Local authorities (and trusts or other organisations delivering statutory children's social care services on behalf of local authorities) are invited to bid to participate in the seventh cohort as part of a regional partnership.

Previously, Step Up was delivered by 136 Local Authorities (LAs), working together via 22 regional partnerships. We expect similar numbers of LAs and regional partnerships to participate in cohort 7. Trainees are based within LAs / regional partnerships which contract with HE providers of social work education to deliver the training element and accredit qualifications. We expect all regional partnerships to take part in cohort 7,

1.3 Business Overview

To meet the business objectives described in the tender specification and support this programme of work, the DfE requires a fully managed service where:

- Information, coordination and administrative support will be provided to local authorities grouped in regional partnerships to assess an anticipated application pool and recruit applicants to the seventh cohort of the Step Up to Social Work programme.

- support will be provided to regional partnerships in planning the recruitment of applicants, via an IT-based application data capture system that will be designed and hosted, with administrative support and staffing function for both stage one application assessment and stage two regional partnership assessment centres.

- The contractor shall perform a dual role in respect of applicants to the programme, namely:

- an ongoing quality assurance function to regional partnerships and DfE on applications and applicant tracking at all stages of the process from appointment through to end of contract.

- as a single, accurate and consistent contact point and source of information for applicants at all stages of the assessment process.

- The contractor is expected to liaise with LAs and regional partnerships across England, in order to coordinate the assessment process and assessment centres. The contractor shall work closely with regional partnerships to provide on-going support before, during and after the assessment process.

- Provide detailed management information to the Department on a weekly, monthly, and ad-hoc basis.

- provide participating regional partnerships with a consistent point of contact via email and telephone for the programme over the life of the contract, from contract award through to the expiry of the contract

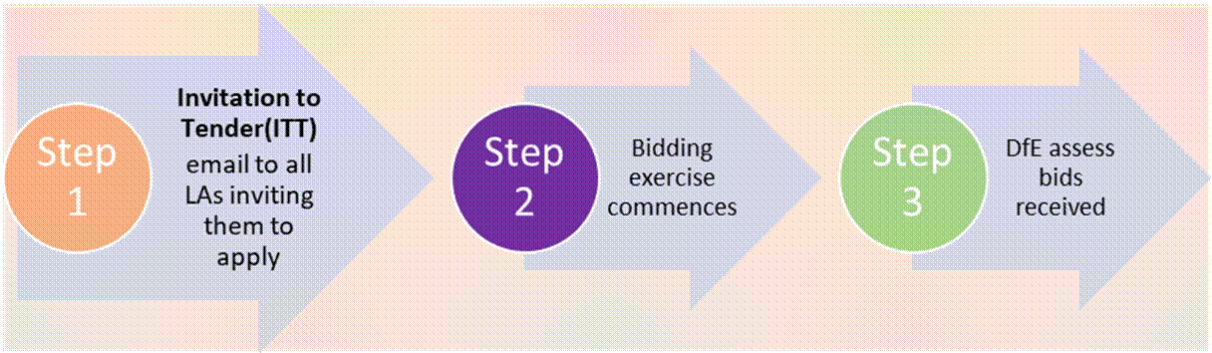
- in collaboration with representatives of regional partnerships and DfE, design and build an appropriate application form for cohort seven candidates

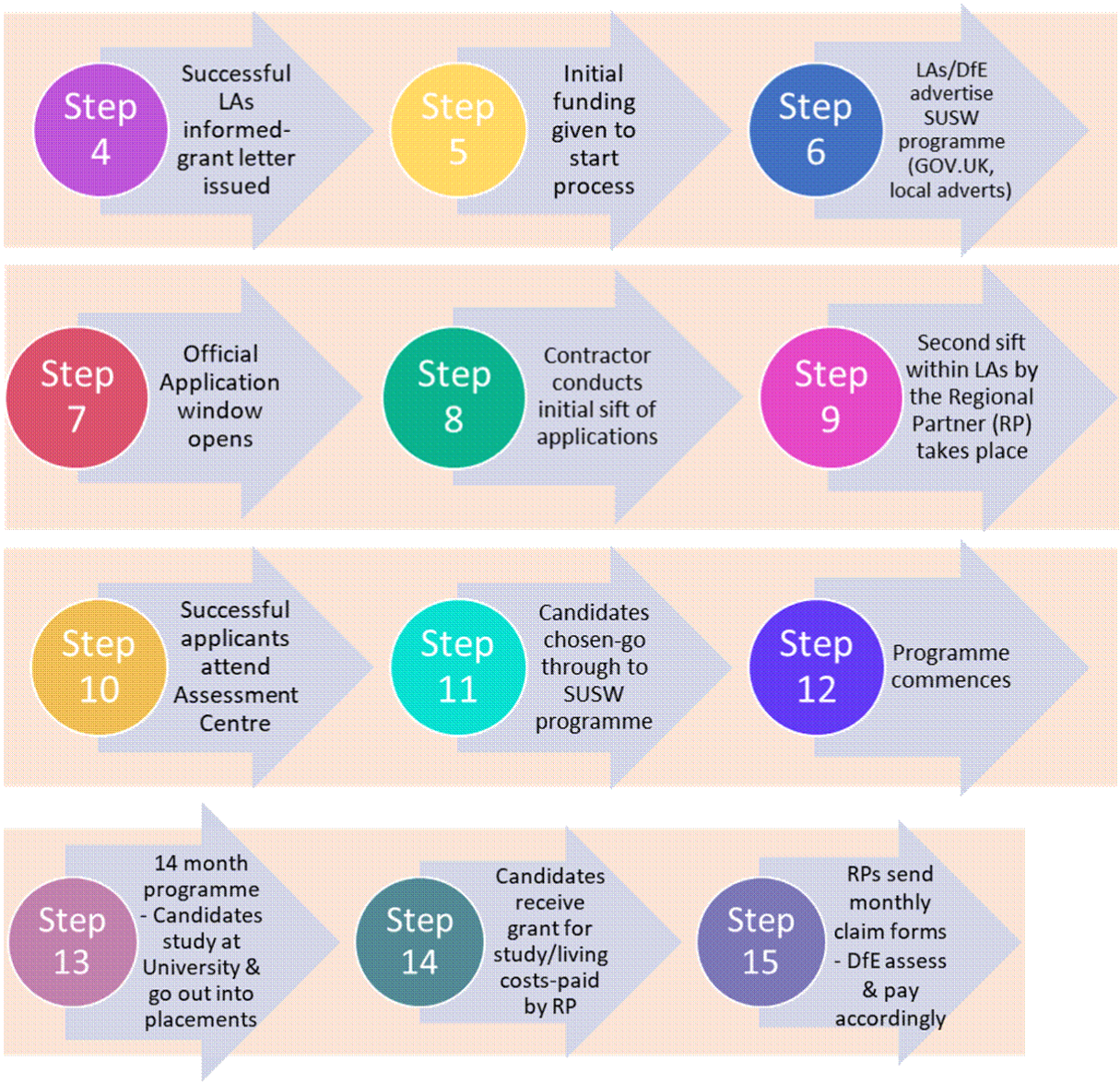
- simultaneously design and build capacity to host cohort seven candidate electronic application data (and manage any potential minority of paper-based applications) to a sufficient level capable of dealing with initial applications.

- in readiness for the cohort seven application window, obtain access to sufficiently trained and knowledgeable resources able to meet the demands of undertaking initial assessment for formal applications to join cohort seven.

The diagram in the following section describes the Step Up process from a high level perspective.

1.4 Step Up Process – High Level View





2. Business Requirements Specification

This section contains the business requirements that shall be met by the bidder's proposed services provision.

2.1 On-boarding

It is imperative that the winning bidder can get the programme up and running once the contract has started, in order to meet the demands of the Department and regional partnerships. There will need to be a plan with clear milestones, deliverables, and the resources you will make available to ensure each task is carried out effectively.

2.1.1 Programme and Project Management

The department requires the bidder to provide timely, accurate, efficient and effective support for the SUSW cohort seven recruitment process. To ensure the appropriate planning is in place, the bidder will need provide an indicative resource plan setting out the key deliverables, timescales etc.

2.2 Administrative and Quality Assurance

The Department requires a solution that will effectively provide information, coordination and administrative support to the regional partnerships as part of the process for cohort seven. There needs to be a plan in place on how the administrative tasks will be sufficiently undertaken, including an ongoing quality assurance function to regional partnerships and the department on applications and applicant tracking at all stages of the process.

2.3 Regional Assessments Centres

The winning bidder will be required to demonstrate how they will provide sufficient and effect resource to support regional partnerships during the second stage of the process. Resourcing must be scalable and appropriate, ensuring both an increase and decrease in demand for resources can be delivered. For example, agreeing with those regional partnerships requesting support, a pre-determined method to clearly and consistently provide each candidate with an explanation of the documentation required for proof of academic achievement - to limit the number of complaints and appeals against the assessment centre process and speed up decision-making. For those regional partnerships requiring administrative assistance at assessment centres the contractor should be prepared to attend a pre-assessment centre visit.

2.4 Resource Capacity & Capability

The DfE's expectation is to procure a fully managed process. The contactor must therefore be capable of effectively delivering the services as specified within this tender, with the necessary resources required to do so.

2.5 Off-boarding

It is imperative that the winning bidder can appropriately scale down resource for delivery of the contract from the end of the assessment centre phase until the end of the contract. This will include the decommissioning of the website and destroying data in line with GDPR. The bidder will need provide an indicative off-boarding (exit) plan to effectively demonstrate how they will bring the required work to a close.

2.6 Reporting Services

So as to monitor the effectiveness of the programme, the DfE will require a variety of reporting. This will include weekly progress reports on number of interested applicants and those who have started/completed applications, regular review meetings with DfE until the assessment centre phase of the contract is completed and acceptances from successful candidates have been received. Thereafter, fortnightly progress reports and review meetings until the anticipated end of contract. Additionally, there may be a need to provide Regional partnership management information sub-sets of data (if required by DfE or partnerships).

2.7 Candidate Tracking and Satisfaction Survey

Suppliers will be responsible for the processing of candidate feedback from local authority regional partnerships to maintain an accurate and up-to-date database. This will enable the Department to continually improve the programme by making the appropriate changes based on user feedback

3. Functional Requirements

This section contains the functional requirements that shall be met by the bidder's proposed solution.

3.1 Solution Design

The Solution Design requirement is not a functional one, but resides here to facilitate easier readability of the functional (and other) requirements which follow, and to assist in the evaluation of the bid responses.

3.2 User Management

The solution will be managed by the supplier, but there may be a need for DfE staff to have access to the solution e.g. to access reporting data. A role-base access approach to user access will therefore be required, with the appropriate security and permissions in place.

3.2.1 User Authentication

In accessing the solution, all users will need to be authenticated using, where possible, two factor authentication. Passwords should be securely stored and encrypted (salted and hashed) and the authentication should be based upon open standards such as SAML 2.0 or OpenID.

3.2.2 Groups and Roles

Within the proposed IT solution, users will need to be assigned specific roles or profiles that determine how they are able to interact with the functionality and services provided – the exact configuration of roles and permissions will need to be agreed with the winning bidder.

3.3 Application Management

To support the successful delivery of the Step Up programme, the supplier will need to provide a fully hosted and managed digital solution that can accommodate the submission, sifting and processing of up to 8,000 applications via an official application form. The details of the application form will be agreed with the winning bidder and developed in collaboration with the regional partnerships and the DfE. The solution must ensure that the application has been validated against the criteria set by the DfE / regional partnerships.

***Note**: the DfE shall own the domain name to be used for the online digital solution.*

3.4 User Self-Service

Applicants should be able to research information about individual regional partnerships via links on the website. These should be available alongside guidance on how to complete and access the form. The expectation here is that all advice and guidance available to the applicants must be easy to find, accessible and in a user-friendly format. This should be delivered as per the requirements below.

3.5 Management Information

So as to monitor the effectiveness of the programme, the DfE will require a variety of reporting.

4. Non-Functional Requirements

This section contains the non-functional requirements that shall be met by the bidder's proposed solution.

4.1 Volumetrics & Resilience

The project requires a solution that will facilitate the storage of data and information that can be added to and analysed year on year.

4.2 Platform, Hosting and Access

The DfE's expectation is to procure a fully managed SaaS solution, and require that

solution to be fully hosted (i.e. Web Application and Data) within the EEA.

4.3 Interoperability

The proposed IT solution must be capable of interfacing and interoperating with other applications, systems and services with the minimum of bespoke development.

4.4 Security

Aside from the legislative compliance, Bidders must ensure that their proposed IT solution is compliant with those data and information security standards, processes and procedures set out by the DfE's Cyber Security unit. The procurement documentation pack contains details of the Cyber Assurance governance processes and the mandatory questionnaire which must be completed by the supplier as part of their bid response – failure to complete this may result in the bidder being excluded from the procurement process

4.5 Open Standards – GDS Compliance

To support the delivery of a fully interoperable solution providing a consolidated platform with data that can be analysed fully within the Department, the proposed IT solution will need to adhere to certain data standards. In addition, the current Cabinet Office and GDS guidance is that all Public Sector IT solutions should, where possible, adopt the use of open standards.

The Technology Code of Practice sets out the guidelines for the delivery of Digital services based on Open standards that offer a common and flexible means by which the Department's suppliers may deploy software tools or functionality. This helps to ensure the maximum level of interoperability between products and services, and suppliers should be able to provide products and services which are either based on open standards, or have the ability to support open standards (such as open source software).

Supporting References: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

4.6 Service Management

To ensure that users of the delivered IT solution is fully supported by the supplier, the following requirements must be met. The over-arching requirement is that suppliers service management processes and procedures must be fully aligned with ITIL v3.

Supporting References: ITIL http://www.itil-officialsite.com

4.7 Accessibility

The DfE requires a solution that will meet the latest industry standards for accessibility. Suppliers must demonstrate that any non-web based applications meet 3 key Departmental Standards:

- Accept Operating System configurations;
- Accept Operating Systems (Windows/Apple/Linux) Accessibility Features; and
- Accept and/or provide short cut keys (this is particularly important for non-web based applications, since they do not have other quick navigation features (such as headings and links) that accessibility users can take advantage of.

Adherence to these standards will give the best possible result. Where supplier products are unlikely to meet all of these standards, suppliers will need to document which elements of their proposed solution would compromise any of the above Department's standards. A list of Assistive Technologies currently used by the Department follows:

- JAWS - A Screen reader and speech synthesizer developed by Freedom Scientific, for use by people who have little or no sight.
- Supernova - A screen magnifier and screen reader developed by Dolphin Systems, for use by people with a range of visual impairments.
- Zoomtext - A screen magnifier and screen reader developed by Al Squared for use by people with a range of visual impairments.
- Dragon - A speech recognition tool developed by Nuance, for use by people with physical and motor impairments (including RSI). Can also help with dyslexia.

End of schedule 1

Schedule 2

Financials

1. Table **[redacted]**

2

End of Schedule 2

Schedule 3a

Processing, Personal Data and Data Subjects

This Schedule shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are**:[redacted]**
2. The contact details of the Processor's Data Protection Officer are **[redacted]**
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Department is the Controller and the Contractor is the Processor in accordance with Clause 17.1 for all activities unless specifically stated in Schedule 3b.
Subject matter of the processing	The processing is needed to ensure that the Processor can effectively deliver the contract to provide the service as described in Schedule 1 (The Specification)
Duration of the processing	The Processing shall only occur during the lifetime of this contract in line with clause 2.1 and 2.2
Nature and purposes of the processing	The nature of the processing is the collection, storage and use of personal data to effectively undertake the purpose of the contract as defined in Schedule 1 (The Specification), including through the sharing of data generated with Regional Partners for their use in providing training opportunities. Any further sharing of this data will be via the anonymisation and aggregation of outcome and output data to inform the Department of the achievement of the Contract.
Type of Personal Data	For applicants: Name Postal address E-mail address Nationality Employment history Details of education and qualifications Diversity data comprising gender, ethnic origin, religious belief, age and disability (including existence of any reasonableness adjustments) For stakeholders within local authorities who are the end employers for successful candidates in the programme: Name Postal address

	E-mail address
Categories of Data Subject	Applicants Stakeholders within local authorities who are the end employers for successful candidates in the programme.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	As per clause 1.15 of Schedule 8 (DFE Security Standards)

Schedule 3b

Joint Controller Agreement

1. For the purpose of this Contract and notwithstanding Clause 17 and Schedule 3a, the Department and the Contractor agree that they are Joint Controllers where Personal Data is processed for the following joint purposes, which shall comprise the **"Agreed Purposes"**:

(a) Identifying suitable candidates
(b) Contractor advertises roles and Department approves content of advert
(c) Contractor identifies suitable candidates based on Department requirements and passes to Department for determination.
(d) Contractor uses their internal IT systems for this collection and processing of candidate Personal Data

Where Personal Data is processed in accordance with the Agreed Purposes, paragraphs 2 - 6 of this Schedule 3b shall apply and, to the extent of any conflict, shall take precedence over Clause 17 and Schedule 3a.

2. For the purposes of paragraphs 3 - 6 below, the following additional capitalised terms shall mean:

"Data Discloser": a party that discloses Shared Personal Data to the other party;

"Permitted Recipients": the parties to this agreement, the employees or officers of each party and, where relevant, any third parties or Sub-contractors engaged to perform or receive the benefit of the Services; and

"Shared Personal Data": the Personal Data to be shared between the parties under paragraph 3 of this Schedule 3b. Shared Personal Data shall be confined to the following categories of information relevant to the following categories of Data Subject: -

Name
Postal address
E-mail address
Nationality
Employment history
Details of education and qualifications
Diversity data, comprising gender, ethnic origin, religious belief, age and disability (including existence of any reasonableness adjustments)

3. Each party acknowledges that the other shall act as a Data Discloser and will regularly disclose to the other party Shared Personal Data collected by the Data Discloser for the Agreed Purposes.

4. Each party shall comply with all the obligations imposed on a Controller under the Data Protection Legislation.

5. Each party shall:

(a) ensure that it has all necessary notices and consents in place to enable lawful transfer of the Shared Personal Data to the Permitted Recipients for the Agreed Purposes. To the extent Shared Personal Data comprises special category data, the Data Disclosure shall ensure that it has in place consent or otherwise a valid condition for processing such data;

(b) give full information to any Data Subject whose Personal Data may be processed under this Schedule 3b of the nature such processing. This includes giving notice that, on the termination of the Contract, Personal Data relating to them may be deleted, transferred to one or more of the Permitted Recipients or their successors or retained in accordance with applicable law;

(c) process the Shared Personal Data only for the Agreed Purposes;

(d) not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients;

(e) ensure that all personnel and officers of the Permitted Recipients who process Personal Data are subject to appropriate obligations of confidentiality;

(f) ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data;

(g) not transfer Personal Data outside of the EU unless the prior written consent of the other party has been obtained and the following conditions are fulfilled:

(i) the party seeking to transfer data has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 45 or LED Article 37);
(ii) the Data Subject has enforceable rights and effective legal remedies; and
(iii) the party seeking to transfer data complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred.

6. Each party shall, subject to paragraph 7 below, assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each party shall:

(a) consult with the other party about any notices given to Data Subjects in relation to the Shared Personal Data;

(b) promptly inform the other party about the receipt of any Data Subject Request or communication from the Information Commissioner (or any other regulatory authority) in connection with Personal Data processed under this Contract;

(c) provide the other party with reasonable assistance in complying with any Data Subject Request or request from the Information Commissioner;

(d) not disclose or release any Shared Personal Data in response to a Data Subject Request without first consulting the other party wherever possible;

(e) assist the other party in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, notifications of a Data Loss Event, completion of Data Protection Impact Assessments and consultations with supervisory authorities or Regulatory Bodies;

(f) notify the other party promptly on becoming aware of any breach of the Data Protection Legislation, and with regard to overall reporting timescales to the Information Commissioner;

(g) at the written direction of the Data Discloser, delete or return Shared Personal Data and copies thereof to the Data Discloser on termination of this Contract unless required by law to store the Personal Data;

(h) use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from Personal Data transfers;

(i) maintain complete and accurate records and information to demonstrate its compliance with this Schedule 3b; and

(j) provide the other party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Legislation, including the procedures to be followed in the event of a Data Loss Event, and the regular review of the parties' compliance with the Data Protection Legislation.

7. Without prejudice to the generality of paragraph 6 above, the parties acknowledge that the Contractor is best placed to receive, and respond to, Data Subject Requests made by applicants in relation to Personal Data collected on their application form and during the initial screen and sift reporting process. It is expected that Data Subject Requests will be made to the general applicant helpline e-mail address and where received in this way the Contractor shall, subject to any need to consult or obtain assistance from the Department, be responsible for responding. Where such requests are instead made to the

Department, the Department shall promptly inform the Contractor in accordance with paragraph 6.

End of Schedule 3

Schedule 4

KPIs, Service Levels and Service Credits

1 The objectives of the KPIs and Service Levels are to:

1.1 ensure that the Services are of a consistently high quality and meet the requirements of the DFE;

1.2 provide a mechanism whereby the DFE can attain meaningful recognition of inconvenience and/or loss resulting from the Contractor's failure to deliver the Services as contracted or in a timely manner; and

1.3 incentivise the Contractor to meet the KPIs and Service Levels and to remedy any failure to meet the KPIs or Service Levels expeditiously.

KEY PERFORMANCE INDICATORS (KPIs) AND SERVICE LEVELS (SLs)

2 This schedule 4 sets out the KPIs (in Table 1) and Service Levels (in Table 2) and designates the **"Performance Measures"** against which the Contractor shall measure its performance.

3 The Contractor shall monitor its performance against each of the KPIs and Service Levels and send the DFE a report detailing the KPIs and Service Levels which were achieved in accordance with the provisions of this schedule 4.

PERFORMANCE MEASURES

4 Throughout the Initial Term (including where extended in accordance with clause 2.2), the Contractor must meet the Performance Measure for each identified KPI as set out in Table 1 below within the agreed **"Service Period"** (which shall mean a calendar month, unless the context requires a longer measurement period to measure compliance against the KPI in which case that period shall take precedence).

5 If during a Service Period the Contractor achieves a KPI, no **"Service Credit"** (which shall mean a reduction in the total amount of charges payable to the Contractor for the corresponding Service Period in accordance with paragraph 9 of this Schedule 4) will accrue to the Contractor in respect of that KPI.

5 The Contractor confirms that it has taken Performance Measures and Service Credits into account in calculating the Charges. Both Parties agree that the Performance Measures and Service Credits are a reasonable method of adjusting the Charges to reflect poor Contractor performance.

7 The Contractor will be expected to meet/comply with all Service Levels as set out within table 2 below, and the Department will consider repeated failures

as breaches of this Contract, but the parties acknowledge that failure to achieve a Service Level shall not attract a Service Credit.

CONSEQUENCES OF FAILURE TO MEET KPIS

8 A failure to meet at least the required Performance Measure will be considered a **"Service Failure"** in respect of the KPIs set out in Table 1 below.

9 If performance level is a Service Failure in one or more of the KPIs listed in Table 1 in any given Service Period, DfE will be entitled at its sole discretion, to reduce the total amount of charges payable to the Contractor for that period/month by: **[redacted]**

10 In addition to its rights under paragraph 9, if there are one or more Service Failures in 3 (three) consecutive Service Periods, the Department will be entitled, as its sole discretion, to terminate this contract on 30 days written notice.

Table 1 KPIs [redacted]

Table 2 Service Levels [redacted]

End of Schedule 4

Schedule 5

Implementation Plan

1. The Contractor shall provide the Services in accordance with the Implementation Plan set out below.

2 The Implementation Plan shall be sufficiently detailed as is necessary to manage the Services and any proposed changes are subject to the Change Control Procedure.

3 The Contractor shall be responsible for implementing and managing the Services and for taking all such steps as may be necessary so as to ensure that from the Service Commencement Date the Contractor is able to provide the Services:

3.1 in accordance with the provisions of the Contract; and

3.2 in a manner that maintains the continuity of Services to the DFE.

4 The Contractor shall monitor its performance against the Implementation Plan and report to the DFE monthly (or more frequently if so required by the DFE)n its performance.

Schedule 6

Change Control Procedure

1 The Parties acknowledge that minor changes to the Contract may be necessary to reflect operational and administrative procedures during the Term and that such minor changes may be agreed in writing between the Parties' respective contract managers. 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.

2 The Contractor shall use reasonable endeavours to incorporate minor changes requested by the DFE within the current Charges and both parties acknowledge they shall not be required to serve a Change Control Note unless the change involves a demonstrable material increase to its costs or requires a material change to the Contract.

3. Either party may request a Variation, provided that such Variation does not amount to a material change, to this Contract by completing a change control note substantially in the form of that set out at Annex 1 to this Schedule 6 (**"Change Control Note"**), including sufficient information to enable to the receiving party to assess the extent of the change and consider whether any amendment to the Charges are required in order to implement the change. If the receiving party accepts the change it shall confirm it in writing within 21 days of receiving the Change Control Note.

4. If the receiving party is unable to accept the change, the matter shall be dealt with in accordance with Clause 23 (Dispute Resolution).

Annex 1 to Schedule 6

Change Control Note

Contract Number		**DFE Contract / Programme Manager**	
Contractor		**Original Contract Value (£)**	
Contract Start Date		**Contract Expiry Date**	

Variation Requested	
Originator of Variation (tick as appropriate)	**DFE** ☐ Contractor ☐
Date	
Reason for Variation	
Summary of Variation (e.g. specification, finances, contract period)	
Date of Variation commencement	
Date of Variation expiry (if applicable)	
Total Value of Variation £ (if applicable)	
Payment Profile (if applicable) e.g. milestone payments	
Revised daily rate (if applicable)	
Impact on original contract (if applicable)	
Supporting Information (please attach all supporting documentation for this Change Control)	
Terms and Conditions	Save as herein amended all other terms and conditions of the Original Contract shall remain in full force and effect.

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	{{Sig_es_:signer1:signature}}	Signature:	{{Sig2_es_:signer2:signature}}
Name:	{{ N_es_:signer1:fullname}}	Name:	{{ N2_es_:signer2:fullname}}

Role:	{{ Ttl_es_:signer1:title}}	Role:	{{ Ttl2_es_:signer2:title}}
Date:	{{ Dte_es_:signer1:date}}	Date:	{{ Dte2_es_:signer2:date}}

Please note that no works/services described in this form should be undertaken, and no invoices will be paid until both copies of the CCN are signed, returned and counter-signed.			
To be entered by the Commercial department:			
Commercial Contact		**Reference Number**	
Date received		**EC Reference**	

End of Schedule 6

Schedule 7

Key Personnel and Key Sub Contractors

Key Personnel

The individuals listed in the table below are Key Personnel:

Name	Role	Period of Involvement

Key Sub-Contractors

The Contractor may sub-contract its obligations under the contract to the Sub-Contractors listed in the table below.

Key Sub-Contractor Name and Address (if not the same as the registered office)	Registered Office and Company Number	Related Product/Service Description	Sub-contract Price expressed as a percentage of total projected Charges over Term	Role in delivery of the Services
NA				

End of Schedule 7

Schedule 8

DFE Security Standards

"BPSS" **"Baseline Personnel Security Standard"**	a level of security clearance described as pre-employment checks in the National Vetting Policy. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
"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. There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers:

https://www.iasme.co.uk/apply-for-self-assessment/

"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 (ITSHC)" **"IT Health Check (ITHC)"** **"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) formerly CESG is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk

“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 The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction
“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. https://www.gov.uk/government/publications/security-policy-framework
”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.
https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology

1.1. The Contractor shall comply with Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

1.2. 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 25 May 2015, 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.

1.3 The Contractor shall demonstrate, and be able to continue to demonstrate, 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).

1.4 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).

1.5 Departmental Data being handled in the course of providing an ICT solution or service must be logically segregated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data 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 1.14.

1.6 The Contractor shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas

1.7 The Contractor shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Departmental Data.

1.8 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.

1.9 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which has been certified to FIPS 140-2 standard or a similar method approved by the Department prior to being used for the transfer of any Departmental Data.

1.10 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 1.11 and 1.12 below.

1.11 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 FIPS140-2 standard or another encryption standard that is acceptable to the Department.

1.12 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 FIPS140-2 standard or another encryption standard that is acceptable to the Department.

1.13 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 disposal organisation.

1.14 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 either visual or physical 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.

1.15 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 and accounted for 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.

1.16 Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.

1.17 All Contractor or sub-contractor employees who handle Departmental Data must have annual awareness training in protecting information.

1.18 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 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, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

1.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data being handled in the course of providing this service, or any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution, shall be investigated immediately and escalated to the Department by a method agreed by both parties.

1.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (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.

1.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any storage of Departmental Data outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management, support or development 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.

1.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service not more than once annually, exclusive of any required follow-up audits required due to issues identified during the course of an annual audit, 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.

1.23 The Contractor shall, where permitted for those arrangements with third party suppliers or sub-contractors which are pre-existing at the Commencement Date, 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.

1.24 The Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA). Any change to these requirements will be dealt with via the change control process as outlined in Schedule 6.

End of Schedule 8

Schedule 9

Commercially Sensitive Information

1. Table 1 and the figure in paragraph 5 of Schedule 2 (Financials)
2. The contents of paragraphs 9.1 to 9.3 of Schedule 4 (KPIs, Service Levels and Service Credits)
3. The Contractor's Implementation Plan set out in Schedule 5 (Implementation Plan)
4. The identities of Key Personnel and their roles set out in Schedule 7 (Key Personnel and Key Sub Contractors)
5. The Contractor's solution in Schedule 10 and, to the extent not contained in Schedule 10, information relating to any Contractor software, proprietary operational processes or methods used in relation to delivery of the Services

Schedule 10

The Contractor's Solution [redacted]