

CONTRACT FOR SCHOOL LEADER TRAINING IN IMPLEMENTING EFFECTIVE FLEXIBLE WORKING PRACTICES

THIS CONTRACT IS DATED 28 APRIL 2021

Parties

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

2) Timewise Solutions Limited, company number 08795991 whose registered office is at Three Tuns House, 109 Borough High Street, London, England, SE1 1NL (“the Contractor”)

Recitals

The Contractor has agreed to provide webinar-based training on implementing flexible working in schools on the terms and conditions set out in this Contract.

The Department's reference number for this Contract is Project 5024.

1 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;

"the Contract Manager"	Name of DfE Contract Manager: Frances Wickstead
"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, Contractors and contractors of the Contractor and/or of any Sub-contractor;
"the Contractor's Contract Manager"	*** name of the Contractor's Contract Manager***
"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", "Processor", "Data Subject", "Personal Data",	take the meaning given in the GDPR

“Personal Data Breach”, “Data Protection Officer”

“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 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 Information" all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and suppliers of the Department, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered to be confidential;

"Department's Intellectual Property Rights" means all Intellectual Property Rights comprised in or necessary for or arising from the performance of the Consultancy Services

"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued 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) 2016/679)
"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
"Law"	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

"LED"	Law Enforcement Directive (Directive (EU) 2016/680)
"Personal Data"	shall have the same meaning as set out in the Data Protection Act 1998;
"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 2003/361/EC and any subsequent revisions.

"Sub-contractor"	the third party with whom the Contractor enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents;
"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

The Contractor shall commence the Services on 28th April 2021 and, subject to Clause 10.1 shall complete the Services on or before 30 April 2022.

The Contract may be extended at the department's discretion up to 6 months subject to satisfactory performance and budget availability.

3 Contractor's Obligations

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

3.2 The Contractor shall comply with the accounting and information provisions of Schedule 2.

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

6 Management

- 6.1** The Contractor shall promptly comply with all reasonable requests or directions of the Contract Manager in respect of the Services.
- 6.2** The Contractor shall address any enquiries about procedural or contractual matters in writing to the Contract Manager. Any correspondence relating to this Contract shall quote the reference number set out in the Recitals to this Contract.

7 Contractor's Employees and Sub-Contractors

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

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

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

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

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

- 7.3** The Contractor shall take all reasonable steps to satisfy itself that its employees or sub-contractors (or their employees) are suitable in all respects to perform the Services.
- 7.4** The Contractor shall 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).
- 7.6** 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 employees or 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.
- 7.10** In addition to any other management information requirements set out in this Contract, the Contractor agrees and acknowledges that it shall, on request and at no charge, provide timely, full, accurate and complete SME Management Information (MI) Reports to the Department including:
- 7.10.1** the total contract revenue received directly on a specific contract;
- 7.10.1** the total value of sub-contracted revenues under the contract (including revenues for non-SMEs/non-VCSEs); and
- 7.10.3** the total value of sub-contracted revenues to SMEs and VCSEs.

8 Intellectual Property Rights - License to the Department

8.1 The Contractor hereby grants to the Department a non-exclusive licence without payment of royalty or other sum by the Department in the Copyright;

8.1.1 to do and authorise others to do any and all acts restricted by the Act as amended from time to time or replaced in whole or part by any statute or other legal means in respect of any Copyright Work created as a result of this contract in the United Kingdom and in all other territories in the world for the full period of time during which the Copyright subsists; and

8.1.2 to exercise all rights of a similar nature as those described in Clause 8.1.1 above which may be conferred in respect of any Copyright Work by the laws from time to time in all other parts of the world

8.2 The Contractor now undertakes to the Department as follows:

8.2.1 not to assign in whole or in part the legal or beneficial title in any Copyright created as a result of this contract to any person, firm or company without the prior written consent of the Department the granting of which consent shall be at its absolute discretion.

8.2.2 to procure that the Contractor is entitled both legally and beneficially to all Copyright.

8.2.3 to record or procure the recording on each and every Copyright Work the name of the author or authors and the date on which it was created and retain safely in its possession throughout the duration of the Copyright all Original Copyright Works.

8.2.4 in respect of the Original Copyright Works to:

8.2.4.1 supply copies on request to the Department the reasonable costs in respect of which the Department will pay; and

8.2.4.2 allow inspection by an authorised representative of the Department on receiving reasonable written notice;

8.2.5 to take all necessary steps and use its best endeavours to prevent the infringement of the Copyright by any person, firm or company which shall include an obligation on the part of the Contractor to commence and prosecute legal proceedings for any threatened or actual infringement where there is a reasonable chance of success and account to the Department after the deduction of all legal expenses incurred in any such proceedings for one half of all damages paid whether by order, settlement or otherwise.

8.2.6 to waive or procure the waiver of any and all moral rights (as created by chapter IV of the Act) of authors of all Copyright Works be waived; and

8.2.7 not to demand and to procure that where any further licences are granted by the Contractor otherwise than to the Department the Licensees thereof do not demand any payment in whatever form and from any person, firm or company directly or indirectly for the undertaking of any of the acts restricted by the Copyright (as defined in section 16 of the Act) in relation to any Copyright Work except in so far as any demand or payment received represents only the reasonable costs which might normally be incurred in respect of such an act.

8.3 The Contractor now warrants to the Department that all Works:

8.3.1 will not infringe in whole or in part any copyright or like right or any other intellectual property right of any other person (wheresoever) and agrees to indemnify and hold harmless the Department against any and all claims, demands, proceedings, damages, expenses and losses including any of a consequential nature arising directly or indirectly out of any act of the Department in relation to any Work, where such act is or is alleged to be an infringement of a third party's copyright or like right or other intellectual property rights (where so ever)

8.4 The warranty and indemnity contained in Clause 8.3.1 above shall survive the termination of this Contract and shall exist for the life of the Copyright.

9 Warranty and Indemnity

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

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

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

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

9.3 The Contractor shall be liable for and shall indemnify the Department in full against any expense, liability, loss, claim or proceedings arising under statute or at common

law in respect of personal injury to or death of any person whomsoever or loss of or damage to property whether belonging to the Department or otherwise arising out of or in the course of or caused by the provision of the Services.

- 9.4** The Contractor shall be liable for and shall indemnify the Department against any expense, liability, loss, claim or proceedings arising as a result of or in connection with any breach of the terms of this Contract or otherwise through the default of the Contractor
- 9.5** All property of the Contractor whilst on the Department's premises shall be there at the risk of the Contractor and the Department shall accept no liability for any loss or damage howsoever occurring to it.
- 9.6** The Contractor shall ensure that it has adequate insurance cover with an insurer of good repute to cover claims under this Contract or any other claims or demands which may be brought or made against it by any person suffering any injury damage or loss in connection with this Contract. The Contractor shall upon request produce to the Department, its policy or policies of insurance, together with the receipt for the payment of the last premium in respect of each policy or produce documentary evidence that the policy or policies are properly maintained.

10 Termination

- 10.1** This Contract may be terminated by either party giving to the other party at least 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. If the breach has not been remedied by the expiry of the specified period, the party not in breach may terminate this Contract with immediate effect by notice in writing.
- 10.3** In the event of a material breach of this Contract by either party, the other party may terminate this Contract with immediate effect by notice in writing.
- 10.4** If any funding from governmental or other sources for the provision of the Services, or for a programme or a project to which the provision of the Services relates is withdrawn, reallocated or no longer available in such a way that the Contract cannot reasonably continue the DFE may terminate the Contract (or any part of it) by serving [30 days] written notice on the Contractor.
- 10.5** If the Authority terminates the Contract in accordance with clause [10.4] the Authority may choose to pay the Contractor reasonable costs in respect of the delivery of the Funded Activities performed up to the termination date. Reasonable costs will be identified by the Contractor and will be subject to the Contractor demonstrating that they have taken adequate steps to mitigate their costs. For the avoidance of doubt, the amount of reasonable costs payable will be determined solely by the Authority.
- 10.6** This Contract may be terminated by the Department with immediate effect by notice in writing if at any time: -

- 10.6.1** the Contractor passes a resolution that it be wound-up or that an application be made for an administration order or the Contractor applies to enter into a voluntary arrangement with its creditors; or
- 10.6.2** a receiver, liquidator, administrator, supervisor or administrative receiver be appointed in respect of the Contractor's property, assets or any part thereof; or
- 10.6.3** 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
- 10.6.4** the Contractor is unable to pay its debts in accordance with Section 123 of the Insolvency Act 1986.
- 10.6.5** there is a change in the legal or beneficial ownership of 50% or more of the Contractor's share capital issued at the date of this Contract or there is a change in the control of the Contractor, unless the Contractor has previously notified the Department in writing. For the purpose of this Sub-Clause 10.4.5 "control" means the power of a person to secure that the affairs of the Contractor are conducted in accordance with the wishes of that person by means of the holding of shares or the possession of voting power.
- 10.6.6** 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
- 10.6.7** 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;
- 10.6.8** 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;
- 10.6.9** the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil its obligations relating to payment of taxes;
- 10.6.10** 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.
- 10.7** 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 Project and who need to know the information, and shall ensure that such Contractor Personnel are aware of and shall comply with these obligations as to confidentiality.

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

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

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

- 12.6.1** on a confidential basis to any Central Government Body for any proper purpose of the Department or of the relevant Central Government Body;
- 12.6.2** to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement;
- 12.6.3** to the extent that the Department (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions;
- 12.6.4** on a confidential basis to a professional adviser, consultant, supplier or other person engaged by any of the entities described in Clause 12.6.1 (including any benchmarking organisation) for any purpose relating to or connected with this Contract;
- 12.6.5** on a confidential basis for the purpose of the exercise of its rights under this Contract, including audit rights, step-in rights and exit management rights; or
- 12.6.6** on a confidential basis to a proposed successor body in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this Contract.
- 12.7** The Department shall use all reasonable endeavours to ensure that any Central Government Body, Contracting Department, employee, third party or Sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to clause 12 is made aware of the Department's obligations of confidentiality.
- 12.8** Nothing in this clause 12 shall prevent either party from using any techniques, ideas or know-how gained during the performance of the Contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of Intellectual Property Rights.
- 12.9** The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Contract is not Confidential Information. The Department shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.
- 12.10** Subject to Clause 12.9, the Contractor hereby gives its consent for the Department to publish the Contract in its entirety, including from time to time agreed changes to the Contract, to the general public.
- 12.11** The Department may consult with the Contractor to inform its decision regarding any redactions, but the Department shall have the final decision in its absolute discretion.
- 12.12** The Contractor shall assist and cooperate with the Department to enable the Department to publish this Contract.

13 Freedom of Information

- 13.1** The Contractor acknowledges that the Department is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and cooperate with the Department to enable the Department to comply with its information disclosure obligations.
- 13.2** The Contractor shall and shall procure that its Sub-contractors shall:
- 13.2.1** transfer to the Department all Requests for Information that it receives as soon as practicable and in any event within two Working Days of receiving a Request for Information;
 - 13.2.2** provide the Department with a copy of all Information in its possession, or power in the form that the Department requires within five Working Days (or such other period as the Department may specify) of the Department's request; and
 - 13.2.3** provide all necessary assistance as reasonably requested by the Department to enable the Department to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.
- 13.3** The Department shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Contract or any other agreement whether any Information is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.
- 13.4** In no event shall the Contractor respond directly to a Request for Information unless expressly authorised to do so by the Department.
- 13.5** The Contractor acknowledges that (notwithstanding the provisions of Clause 13) the Department may, acting in accordance with the Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 ("**the Code**"), be obliged under the FOIA, or the Environmental Information Regulations to disclose information concerning the Contractor or the Project:
- 13.5.1** in certain circumstances without consulting the Contractor; or
 - 13.5.2** following consultation with the Contractor and having taken their views into account;
- provided always that where 13.5.1 applies the Department shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Contractor advanced notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.
- 13.6** The Contractor shall ensure that all Information is retained for disclosure and shall permit the Department to inspect such records as requested from time to time.

14 Access and Information

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

15 Transfer of Responsibility on Expiry or Termination

- 15.1** The Contractor shall, at no cost to the Department, promptly provide such assistance and comply with such timetable as the Department may reasonably require for the purpose of ensuring an orderly transfer of responsibility upon the expiry or other termination of this Contract. The Department shall be entitled to require the provision of such assistance both prior to and, for a reasonable period of time after the expiry or other termination of this Contract.
- 15.2** Such assistance may include (without limitation) the delivery of documents and data in the possession or control of the Contractor which relate to this Contract, including the documents and data, if any, referred to in the Schedule.
- 15.3** The Contractor undertakes that it shall not knowingly do or omit to do anything which may adversely affect the ability of the Department to ensure an orderly transfer of responsibility.

16 Tax Indemnity

- 16.1** Where the Contractor is liable to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration. Where the Department has deemed the Contractor to be an Off-Payroll Contractor as defined by Her Majesty's Revenue and Customs the Department reserves the right to calculate Income Tax and pay it to HMRC. The amounts will be deducted from the Contractor's fee for the work provided.
- 16.2** Where the Contractor is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration. Where the Department has deemed the Contractor to be an Off-Payroll Contractor as defined by Her Majesty's Revenue and Customs the Department reserves the right to calculate primary (employee) National Insurance contributions (NICs) and pay them to HMRC. The amounts will be deducted from the Contractor's fee for the work provided.
- 16.3** The Department may, at any time during the term of this contract, ask the Contractor to provide information which demonstrates how the Contractor complies with Clauses 16.1 and 16.2 above or why those Clauses do not apply to it.
- 16.4** A request under Clause 16.3 above may specify the information which the Contractor must provide and the period within which that information must be

provided.

16.5 The Department may terminate this contract if-

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

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

or

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

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

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

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

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

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

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

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

17 Data Protection

- 17.1** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Schedule 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:
- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
 - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) 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:
- (a) 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;
 - (b) 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;
 - (c) 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
- (d) 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 46 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;
- (e) 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 17.6, the Processor shall notify the Controller immediately if it:

- (a) receives a Data Subject Request (or purported Data Subject Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
- (e) 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
- (f) 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 full assistance in relation to either Party's obligations under Data Protection Legislation 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:

- (a) the Controller with full details and copies of the complaint, communication or request;
- (b) 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;
- (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Controller following any Data Loss Event;
- (e) 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:

- (a) the Controller determines that the processing is not occasional;
- (b) 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
- (c) 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:

- (a) notify the Controller in writing of the intended Sub-processor and processing;
- (b) obtain the written consent of the Controller;
- (c) 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
- (d) 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.

18. Departmental Security Standards for Business Services and ICT Contracts

<p>"BPSS"</p> <p>"Baseline Personnel Security Standard"</p>	<p>means the Government's HMG Baseline Personal Security Standard . Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard</p>
<p>"CCSC"</p> <p>"Certified Cyber Security Consultancy"</p>	<p>is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards.</p> <p>See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy</p>
<p>"CCP"</p> <p>"Certified Professional"</p>	<p>is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme</p>
<p>"CPA"</p> <p>"Commercial Product Assurance"</p> <p>[formerly called "CESG Product Assurance"]</p>	<p>is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa</p>
<p>"Cyber Essentials"</p> <p>"Cyber Essentials Plus"</p>	<p>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.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body</p>
<p>"Data"</p> <p>"Data Controller"</p> <p>"Data Protection Officer"</p> <p>"Data Processor"</p> <p>"Personal Data"</p> <p>"Personal Data requiring Sensitive Processing"</p> <p>"Data Subject", "Process" and "Processing"</p>	<p>shall have the meanings given to those terms by the Data Protection Act 2018</p>
<p>"Department's Data"</p> <p>"Department's Information"</p>	<p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including:</p>

	<p>(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:</p> <ul style="list-style-type: none"> (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 <p>(b) any Personal Data for which the Department is the Data Controller;</p>
<p>“DfE” “Department”</p>	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 / G-Cloud”	means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
End User Devices	means the personal computer or consumer devices that store or process information.
<p>“Good Industry Practice” “Industry Good Practice”</p>	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.
<p>“Good Industry Standard” “Industry Good Standard”</p>	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.
<p>“GSC” “GSCP”</p>	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) and 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"	means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"NCSC"	The National Cyber Security Centre (NCSC) is the UK government's National Technical Authority for Information Assurance. 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). the term 'OFFICIAL-SENSITIVE' 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 GSCP.
"RBAC" "Role Based Access Control"	means Role Based Access Control. A method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"Secure Sanitisation"	means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can 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"	means 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
“Senior Information Risk Owner” “SIRO”	means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
“SPF” “HMG Security Policy Framework”	means 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

18.1. The Contractor shall be aware of and comply the relevant [HMG security policy framework](#), [NCSC guidelines](#) and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.

- (Guidance: Providers on the HMG Digital Marketplace / GCloud that have demonstrated compliance, as part of their scheme application, to the relevant scheme’s security framework, such as the HMG Cloud Security Principles for the HMG Digital Marketplace / GCloud, may on presentation of suitable evidence of compliance be excused from compliance to similar clauses within the DfE Security Clauses detailed in this section (Section 12).)

18.2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of [Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14](#) dated 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and will be expected to retain certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

- (Guidance: Details of the acceptable forms of equivalence are stated at Section 9 of Annex A within the link to Cabinet Office document in this clause).
- (Guidance: The Department’s expectation is that the certification scope will be relevant to the services supplied to, or on behalf of, the Department. However, where a contractor or (sub) contractor is able to evidence a valid exception or certification to an equivalent recognised scheme or standard, such as ISO 27001, then certification under the Cyber Essentials scheme could be waived. Changes to the Cabinet Office Action Note will be tracked by the DfE)

- (Guidance: The department's expectation is that SMEs or organisations of comparable size shall be expected to attain and maintain Cyber Essentials. Larger organisations or enterprises shall be expected to attain and maintain Cyber Essentials Plus.)

18.3 Where clause 12.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

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

- (Guidance: The Department's expectation is that suppliers claiming certification to ISO/IEC 27001 shall provide the Department with copies of their Scope of Certification, Statement of Applicability and a valid ISO/IEC 27001 Certificate issued by an authorised certification body. Where the provider is able to provide a valid Cyber Essentials certification then certification under the ISO/IEC 27001 scheme could be waived and this clause may be removed.)

18.4 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 all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

- (Guidance: The Department's expectations are that all contractors shall handle the Department's information in a manner compliant with the GSCP. Details of the GSCP can be found on the GOV.UK website at: <https://www.gov.uk/government/publications/government-security-classifications>.)
- (Guidance: Compliance with the GSCP removes the requirement for the department to issue a Security Aspects Letter (SAL) to the contractor).

18.5 Departmental Data being handled in the course of providing an ICT solution or service must be separated 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 line with clause 12.14.

- (Guidance: Advice on HMG secure sanitisation policy and approved methods are described at <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>)

- 18.6** The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.
- (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)
- 18.7** The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.
- (Guidance: Where the contractor's and sub-contractor services are wholly carried out within Departmental premises and all access to buildings or ICT systems is managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

18.8 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 processes;
- malware protection;
- boundary access controls including firewalls;
- maintenance and use of fully supported software packages in accordance with vendor recommendations;
- software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
- user access controls, and;
- the creation and retention of audit logs of system, application and security events.

(Guidance: Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources or locations managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

18.9 The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

18.10 The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.

(Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the use of removable media as described in this clause is either prohibited or not required in order to deliver the service this clause shall be revised as follows: - 'The use of removable media in any form is not permitted'.)

18.11 The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at:

<https://www.ncsc.gov.uk/guidance/end-user-device-security> and
<https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles>.

(Guidance: The use of an encryption product that utilises the AES256 algorithm would be considered 'industry good practice' in this area. Where the contractor's and sub-contractor services are wholly carried out using Departmental ICT resources managed directly by the Department as part of the service, the Department shall be responsible for meeting the requirements of this clause.)

- 18.12** 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.

The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

- (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at:
<https://www.cpni.gov.uk/secure-destruction>)

- 18.13** 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.

The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

- 18.14** In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.

- (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning sanitisation must be in accordance with guidance provided by NCSC and CPNI.

- 18.15** In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

- (Guidance: Where there is no acceptable secure sanitisation method available for a piece of equipment, or it is not possible to sanitise the equipment due to an irrecoverable technical defect, the storage media involved shall be destroyed using an HMG approved method described at <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>.)
- (Guidance: Further advice on appropriate destruction and disposal methods for physical and hardcopy documents can be found at: <https://www.cpni.gov.uk/secure-destruction>)
- (Guidance: The term 'accounted for' means that assets and documents retained, disposed of or destroyed should be listed and provided to the department as proof of compliance to this clause.)

- 18.16** Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, 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. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.

- (Guidance: Further details of the requirements for HMG BPSS clearance are available on the website at: <https://www.gov.uk/government/publications/government-baseline-personnel-security-standard>)
- (Guidance: Further details of the requirements for National Security Vetting, if deemed necessary for this contract are available at: <https://www.gov.uk/government/publications/hmg-personnel-security-controls>)

- 18.17** All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.
- 18.18** 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.
- (Guidance: The business continuity and disaster recovery plans should be aligned with industry good practice and it is the Department's expectation that all vendors providing services or infrastructure to the Department will have plans that are aligned to the ISO 22301 standard in place. Further information on the requirements of ISO 22301 may be found in the standard.)

- 18.19** Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department's nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

- 18.20** 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 an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

- (Guidance: Further information on IT Health Checks and the NCSC CHECK Scheme which enables penetration testing by NCSC approved companies can be found on the NCSC website at:
<https://www.ncsc.gov.uk/scheme/penetration-testing>.)

18.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.

(Guidance: The offshoring of HMG information outside of the UK is subject to approval by the Departmental SIRO).

18.22 The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.

18.23 The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. 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 Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.

- (Guidance: It is Departmental policy that suppliers of business services shall provide evidence of an acceptable level of security assurance concerning their organisation. Further advice and guidance on the Department's security assurance processes can be supplied on request. Information about the HMG Supplier Assurance Framework can be found at:
<https://www.gov.uk/government/publications/government-supplier-assurance-framework>
- (Guidance: Further information on the CCP and CCSC roles described above can be found on the NCSC website at: <https://www.ncsc.gov.uk/information/about-certified-professional-scheme> and <https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy>)

18.24 Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:

- Compliance with HMG Minimum Cyber Security Standard.
- Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
- Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any

caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

18.25 The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.

19 Amendment and variation

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

20 Assignment and Sub-contracting

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

21 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.

22 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.

23 Notices

23.1 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).

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

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

23.2.2 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;

23.2.3 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).

24 Dispute resolution

24.1 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.

24.2 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.

24.3 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.

25 Discrimination

25.1 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.

25.2 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.

26 Law and Jurisdiction

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

As witness the hands of the parties

Authorised to sign for and on
behalf of the Secretary of
State for Education

Signature

Name: [REDACTED]

Position in Organisation:
Deputy Director

Address in full:
Department for Education
Sanctuary Buildings
Great Smith Street
London, SW1P 3BT

Date: 28th April 2021

Authorised to sign for and on
behalf of Timewise Solutions Limited

Signature

Name in [REDACTED]

Position in Organisation:
Development Director

Address in full:
Three Tuns House, 109 Borough
High Street, London SE1 1NL

Date: 28th April 2021

1 Background

- 1.1 Flexible working practices can help to recruit, retain and motivate teachers and can play a central role in helping schools to deploy their staff effectively and efficiently. Supporting schools to implement flexible working and removing challenges to flexible working forms a core part of the DfE's Teacher Recruitment and Retention Strategy.
- 1.2 Some teachers leave the profession or choose not to return to teaching because they cannot access flexible working opportunities. Evidence shows that among secondary school teachers who leave the profession, the proportion who take up part-time positions elsewhere increases by 20 percentage points after leaving, suggesting an unmet demand for flexible working, particularly in secondary schools.¹
- 1.3 This training offer will form part of our overall strategy to increase flexible working in schools.
- 1.4 DfE includes in its definition of flexible working formal changes to working patterns (job sharing, part-time, compressed hours and other changes to the time and place that work is carried out) as well as ad hoc flexibility such as the ability for staff to take a personal day and time in lieu.
- 1.5 DfE is encouraging schools to adopt a whole-school or strategic approach where school leaders design organisational culture and systems to accommodate the flexibility their staff need, rather than respond as and when individual requests arise. A key part of this is to have a policy on flexible working which includes information such as the types of flexible working available, and the procedures for making a request. This should be proactively communicated to staff in order to ensure that staff and the employer can work together to accommodate flexible working requests wherever possible.
- 1.6 DfE recognises the primary decision makers to be a school or MAT's school leadership team (SLT), their school business professions (SBPs) or HR business support, and governors/trustees. Therefore we are requiring the Contractor to provide tailored training to these three groups.

2 Aim

- 2.1 The Contractor shall use all reasonable endeavours to achieve the following aims:
 - to offer education-specific training on flexible working practices in schools that is free to participants and open to participants from all schools nationally;
 - to provide content tailored to various decision-makers in schools, including school leaders/MAT leaders, SBPs and governors/trustees; and
 - to deliver practical content on how to design and implement a strategic or 'whole school' approach to flexible working for staff in schools. This content should be reflective of schools' specific HR needs, which will enable participants to translate their learning into an increased flexible working offer to school staff.

¹ Bamford and Worth, 2017; Sharp et al., 2019

3 Objectives

3.1 The Contractor shall use all reasonable endeavours to achieve the following objectives:

- improved knowledge on how to manage and respond to flexible working requests;
- improved knowledge on how to implement different types of flexible working; and
- increased intention to improve their school or trust's flexible working offer to staff.

These will be measured by post-webinar surveys, analysed by DfE, as well as monthly reports from the contractor.

In the longer term we expect to see in participants' schools:

- more schools putting in place flexible working policies;
- an increased number of jobs advertised as 'flexible'; and
- more teachers in flexible roles.

4 Methodology

The Contractor shall perform the tasks detailed in the Schedule of Work.

SCHEDULE OF WORK

Task /Activity	Requirements	Date Required
<p>Design and create course content and agree this with the Department prior to delivery.</p> <p>Related KPI: design and create course content.</p>	<p>The webinar content must take into account views from key DfE stakeholders:</p> <ul style="list-style-type: none"> • This will include members of the Flexible Working Advisory Group and Flexible Working Ambassador Schools (FWAS) • Process regarding how to seek views from DfE stakeholders to be agreed with DfE and may include attendance at Flexible Working Advisory Group meeting and Flexible Working Ambassador Schools project launch meeting. • DfE to facilitate engagement with Advisory Group and FWAS. <p>As detailed in Timewise's bid, content to reflect:</p> <div data-bbox="779 810 1933 1374" style="background-color: black; width: 100%; height: 350px; position: relative;"> <div style="position: absolute; top: 50px; left: 50px; width: 80%; height: 80%;"></div> </div>	<p>April 2021 - June 2021.</p> <p>(content may also be developed on ongoing basis in response to feedback May 2021-Feb 2022)</p>

	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>Content to also take into account the different requirements for each of the three groups. As set out in Timewise's bid, this will include:</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
Task /Activity	Requirements	Date Required
Deliver agreed number of webinars across at least two academic terms	<p>The delivery model for project to be as follows:</p> <ul style="list-style-type: none"> • Three live webinars hosted on Zoom. • Webinars to be recorded and uploaded to private Youtube site. Recordings 	June/July 2021 to February/

<p>Related KPI: To deliver at least 14 training episodes in accordance with agreed delivery model</p>	<p>also to be made available to DfE.</p> <ul style="list-style-type: none"> • Live webinars to last: <ul style="list-style-type: none"> ○ 90 min for School Heads and MAT leaders ○ 90 min for HR/Business professionals ○ 60 min for Governors/Trustees. • Three follow-up clinics. • Eight interactive drop-in clinics. • Contribution to flexible working community of practice through thought leadership and representation at ad-hoc events with DfE stakeholders such as LGA, ISBL, FWAS, NGA etc. <p>Webinar delivery to include:</p> <ul style="list-style-type: none"> • Content to cover the topics detailed above and include the following resources: <ol style="list-style-type: none"> 1. Key guest speakers, including school leaders who excel in this area to persuade other schools of the opportunity to change. 2. Polls and Q&A functionality to ensure the session is interactive. 3. Recording and dissemination through the provider's partner networks, where appropriate. 4. The follow-up Q&A clinics to be focused on the different audience groups, based on participant feedback and needs. These will be designed to go deeper into specific topics, allowing participants to bring their questions and issues to the table and to provide practical tools and guidance 5. Eight interactive drop in clinics. <p>The delivery of webinars will include:</p> <ul style="list-style-type: none"> • Presentations from Timewise consultants and partner contributors. 	<p>March 2022.</p>
--	--	---------------------------

	<ul style="list-style-type: none"> • Break-out sessions & short diagnostic exercises to help participants self-reflect. • Expert panel discussions. • Case study presentations. <p>Tools provided to accompany the webinars will include:</p> <ul style="list-style-type: none"> • A framework for a change roadmap. • Flexible job design options. • Case studies. • Guidance and trouble-shooting FAQs in the form of slide packs. <p>Accessibility</p> <ul style="list-style-type: none"> • Participants can use any device to participate via Zoom and their own broadband connection. <p>Metrics</p> <ul style="list-style-type: none"> • Registration page to be created by the provider for people to provide details before accessing the webinars or recordings. • People will only be able to access the recordings through the registration process so the provider can provide anonymised information about who is watching the recordings. <p>Contribution to Flexible Working Community of Practice to include:</p> <ul style="list-style-type: none"> • Attendance at events and conferences hosted by DfE stakeholders to promote flexible working. • Opportunities to be shared by DfE on an ad-hoc basis. • Timewise to report on activity. 	
Task /Activity	Requirements	Date Required
	As set out in Timewise's bid - target approximately 400 school leaders, 400 HR/business specialists and 200 governors. Timewise to engage with the newly	June/July 2021 to

<p>Reach expected number of participants and schools.</p> <p>Related KPI: Enrol at least 1000 participants, reaching at least 500 schools (exact number to be agreed during contracting).</p>	<p>appointed Flexible Working Ambassador Schools on raising awareness of flexible working/promoting webinars to teachers/school leaders.</p> <p>Messaging for the different target groups to include the following:</p> <ul style="list-style-type: none"> • Flexible working is a workforce trend that has been accelerating across different sectors of the economy. Employers are no longer asking why they should do it but how. • The importance of embracing flexible working in the context of Covid-19 and why it is more important now than ever. • Flexible working in the school environment presents its own opportunities and challenges. The latter are both operational and attitudinal and can be overcome. This may include addressing resistance from parents and/or school governors. • A reactive approach, in which it is up to people to ask, creates limited opportunities for flexible working; a proactive, whole-school approach is characterised by an open and supportive culture, and processes and skills which enable more flexibility. • These webinars and clinics to provide learnings from experienced practitioners, as well as practical guidance and tools to challenge and support change. • Flexible working is increasingly accepted as key to attracting and retaining a talented and committed workforce. • Targeting to consider strategy for engaging and generating interest among groups who have never considered Flexible Working as a positive step. • Explore other routes for raising awareness, e.g. inclusion of Teacher Vacancies Services information in Timewise's flexible working training material, linking up with the work the DfE Teaching Vacancies marketing team will be doing to promote the benefits of flexible working. <p>Monitor webinar registration on an ongoing basis and adjust marketing and messaging accordingly.</p>	<p>February 2022</p>
--	--	-----------------------------

Task /Activity	Requirements	Date Required
<p>Disseminate and collect initial and longer-term feedback surveys to webinar participants.</p> <p>Related KPIs:</p> <ul style="list-style-type: none"> • A minimum of 70% of participants to complete an initial feedback survey. • 80% rate the course at least 'satisfactory'. • 50% rate the course at least 'good'. • A minimum of 80% of participants who have completed the initial feedback survey to provide positive feedback on course content and delivery. • A minimum of 70% of participants who have completed the initial feedback survey to confirm that they plan to take action to improve flexible working opportunities in their school. 	<p>Feedback survey for participants to be designed by Timewise and agreed with the Department prior to delivery:</p> <ul style="list-style-type: none"> • Feedback surveys to include a measure of how helpful the training has been in addressing challenges surrounding the implementation of flexible working in schools and perceptions of participants relating to flexible working in the education sector. • Initial feedback survey to include a measure participants' intention to implement change following the training. • Longer-term feedback survey to measure action taken to improve flexible working practices since participating in training. <p>As detailed in Timewise's bid, the following steps to be taken to encourage completion of surveys so as to achieve 70% response rate:</p> <ul style="list-style-type: none"> • Undertaking polls during webinars to elicit immediate responses. • Sending out the survey immediately after the event and with consideration for timing. The provider to connect the survey page to Zoom so that when people log out of the webinar they are taken straight to the survey. • Keeping the design very short and being clear in invitations how long it will take. • After the webinars, participants to be asked about what specific topics they would like to cover in the clinics so they can feed in their ideas. • Provider to monitor webinar registration on an ongoing basis and adjust their marketing and messaging accordingly. Survey responses will be managed as per above. • Provide outcome of post event feedback to DfE. • Produce a summary report for both the post event surveys and the longer-term surveys. 	<p>June/July to February 2022 for initial feedback surveys</p> <p>Longer term feedback surveys February – April 2022</p>

--	--	--

Task /Activity	Requirements	Date Required
<p>Engage regularly with the DfE to review KPIs and discuss ongoing issues.</p>	<p>Timewise to:</p> <ul style="list-style-type: none"> • Regularly review the KPIs in line with the project timeline. • Reviewing webinar content with the DfE to be scheduled in as a specific activity. • Monitor webinar registration on an ongoing basis and adjust marketing and messaging accordingly. • Ensure that any risks to the delivery of requirements are recorded with contingencies identified to address any risks that materialise, and, monitor the risks on an ongoing basis. • Engage in monthly reviews and fortnightly phone calls with the DfE to review progress with delivery/KPIs. This will involve completion of a monthly report template. • Report on monthly basis on contribution to flexible working community of practice through Timewise's ad-hoc engagement with DfE stakeholders and participation at awareness raising events. • Attend meetings arranged by the DfE to discuss progress. These will be held at least quarterly and may be more frequently, e.g. monthly depending on progress. <p>To support delivery, and as detailed in their bid, Timewise to:</p> <ul style="list-style-type: none"> • Draw on the necessary expertise to manage the programme and deliver the webinars and run the clinics. • Work with stakeholders, relating to Timewise and the DfE on targeting of the different audience groups across a range of school types at national level. • Analyse feedback from the webinars to inform the content and focus of the clinics. 	<p>April 2021 until March 2022 (summary reports to be produced by April 2022).</p>

End of schedule 1

Schedule 2

1 Table

(OBJ)

Cost Matrix

VAT will be payable at the prevailing rate

- 2 Funds allocated to a particular expenditure heading in the table at paragraph 1 ("the Table") are available for that expenditure heading only. Funds allocated to a particular accounting year are available for that accounting year only. The allocation of funds in the Table may not be altered except with the prior written consent of the Department.
- 3 The Contractor shall maintain full and accurate accounts for the Service against the expenditure headings in the Table. Such accounts shall be retained for at least 6 years after the end of the financial year in which the last payment was made under this Contract. Input and output VAT shall be included as separate items in such accounts.
- 4 The Contractor shall permit duly authorised staff or agents of the Department or the National Audit Office to examine the accounts at any reasonable time and shall furnish oral or written explanations of the account if required. The Department reserves the right to have such staff or agents carry out examinations into the economy, efficiency and effectiveness with which the Contractor has used the Department's resources in the performance of this Contract.
- 5 Invoices shall be prepared by the Contractor and shall be detailed against the expenditure headings set out in the cost matrix. Payment will be in arrears, in three tranches linked to deliverables: [REDACTED]

The Contractor or its nominated representative or accountant shall certify on the invoice that the amounts claimed were expended wholly and necessarily by the Contractor on the Service in accordance with the Contract and that the invoice does not include any costs being claimed from any other body or individual or from the Department within the terms of another contract.

- 6 The Department shall accept and process for payment an electronic invoice submitted for payment by the Contractor where the invoice is undisputed and where it complies with the standard on electronic invoicing. For the purposes of this paragraph, an electronic invoice complies with the standard on electronic invoicing where it complies with the European standard and any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870.
- 7 Invoices shall be sent within 15 days of the end of the relevant month electronically by email to [REDACTED], quoting the Contract

reference number. To request a statement, please email

[REDACTED], quoting the Contract reference number.

The Department undertakes to pay correctly submitted invoices within 5 days of receipt. The Department is obliged to pay invoices within 30 days of receipt from the day of physical or electronic arrival at the nominated address of the Department. Any correctly submitted invoices that are not paid within 30 days will be subject to the provisions of the Late Payment of Commercial Debt (Interest) Act 1998. A correct invoice is one that: is delivered in timing in accordance with the contract; is for the correct sum; in respect of goods/services supplied or delivered to the required quality (or are expected to be at the required quality); includes the date, supplier name, contact details and bank details; quotes the relevant purchase order/contract reference and has been delivered to the nominated address. If any problems arise, contact the Department's Contract Manager. The Department aims to reply to complaints within 10 working days. The Department shall not be responsible for any delay in payment caused by incomplete or illegible invoices.

- 8** The Contractor shall have regard to the need for economy in all expenditure. Where any expenditure in an invoice, in the Department's reasonable opinion, is excessive having due regard to the purpose for which it was incurred, the Department shall only be liable to reimburse so much (if any) of the expenditure disallowed as, in the Department's reasonable opinion after consultation with the Contractor, would reasonably have been required for that purpose.
- 9** If this Contract is terminated by the Department due to the Contractor's insolvency or default at any time before completion of the Service, the Department shall only be liable under paragraph 1 to reimburse eligible payments made by, or due to, the Contractor before the date of termination.
- 10** On completion of the Service or on termination of this Contract, the Contractor shall promptly draw-up a final invoice, which shall cover all outstanding expenditure incurred for the Service. The final invoice shall be submitted not later than 30 days after the date of completion of the Service.
- 11** The Department shall not be obliged to pay the final invoice until the Contractor has carried out all the elements of the Service specified as in Schedule 1.
- 12** It shall be the responsibility of the Contractor to ensure that the final invoice covers all outstanding expenditure for which reimbursement may be claimed. Provided that all previous invoices have been duly paid, on due payment of the final invoice by the Department all amounts due to be reimbursed under this Contract shall be deemed to have been paid and the Department shall have no further liability to make reimbursement of any kind.

End of Schedule 2

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 Customer is the Controller and the Contractor is the Processor in accordance with Clause 17.1.
Subject matter of the processing	Data relating to participants' engagement in providers' programme of webinars and follow up clinics.
Duration of the processing	April 21 to April 22.
Nature and purposes of the processing	<p>The processing is needed to ensure the provider have met KPIs, to evaluate the impact of the project and the performance of the provider.</p> <ul style="list-style-type: none"> • Collection, recording and storing of names, addresses, job role, phase/type of school and region • Collection, storage and transmission of feedback surveys on ongoing basis. <p>Collection, storage and transmission of an end of project / feedback survey to be completed by the provider, based on the surveys collected during the life of the project.</p>
Type of Personal Data	Personal data such as Name, job role, phase/type of school, region, will be collected by survey electronically.
Categories of Data Subject	Education sector: Senior leaders, School Governors, HR professionals.

<p>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</p>	<p>Data shall be returned to DfE securely and to be made accessible by Excel.</p> <p>Data shall be securely destroyed within one year of project completion.</p>
---	--