

CONTRACT FOR DESIGNATED SAFEGUARDING LEAD (DSL) ONLINE RESOURCE

THIS CONTRACT IS MADE ON THE DATE OF SIGNATURE

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) **Virtual College Ltd, registration number 3052439 whose registered office is at Marsel House Stephenson's Way Ilkley West Yorkshire LS29 8DD (“the Contractor”)**

Recitals

The Contractor has agreed to develop a set of online resources to support Designated Safeguarding Leads on the terms and conditions set out in this Contract.

The Department's reference number for this Contract is **con_12318**.

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;

 Department for Education, Piccadilly Gate,
Store Street, Manchester, M1 2WD

“the Contract Manager”

"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 Contractors Contract Manager"	*** [REDACTED], 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", "Personal Data Breach", "Data Protection Officer"	take the meaning given in the GDPR
"Crown"	means Queen Elizabeth II and any successor
"Crown Body"	any department, office or agency of the Crown;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.
"DPA 2018"	Data Protection Act 2018
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.
"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of

	personal data and privacy; (iiii) 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

- 2.1** The Contractor shall commence the Services on 15 December 2021 and, subject to Clause 10.1 shall complete the Services on or before 31 July 2022.
- 2.2** In the event that provisions of clause 5 apply, the Contract may be extended by a further 6 months subject to satisfactory performance.

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 Departments Obligations

The Department will comply with the payment provisions of Schedule 2 provided that the Department has received full and accurate information and documentation as required by Schedule 2 to be submitted by the Contractor for work completed to the satisfaction of the Department.

5 Changes to the Department's Requirements

- 5.1** The Department shall notify the Contractor 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.

8 Intellectual Property Rights

- 8.1** It is acknowledged and agreed between the parties that all existing or future Department's Intellectual Property Rights shall vest in the Crown absolutely.
- 8.2** Any Intellectual Property Rights of the Contractor or Sub-Contractor which are in existence at the date of this Contract and which are comprised in or necessary for or arising from the performance of the Consultancy Services owned by the Contractor ("**Background Intellectual Property**") shall remain in the ownership of the Contractor but in consideration of the fees payable pursuant to this Contract, the Contractor hereby grants to the Department in respect of such Background Intellectual Property an irrevocable, non-exclusive, royalty-free, perpetual licence with rights to grant sub-licences.
- 8.3** The Contractor agrees that at the request and cost of the Department it will and procure that its officers, employees and agents will at all times do all such reasonable acts and execute all such documents as may be reasonably necessary or desirable to ensure that the Department receives the full benefit of all of its rights under this Contract in respect of the Department's Intellectual Property Rights or to assist in the resolution of any question concerning the Intellectual Property Rights.
- 8.4** The Contractor hereby waives any Moral Rights as defined at Chapter IV of the Copyright, Designs and Patents Act 1988.
- 8.5** The Contractor warrants:
- 8.5.1** that the Department's Intellectual Property Rights comprise the original work of and were created by or on behalf of the Contractor;
 - 8.5.2** that the Department's Intellectual Property Rights have not and will not be copied wholly or in part from any other work or material;
 - 8.5.3** That the use of or exercise by the Department of the Department's Intellectual Property Rights and the Background Intellectual Property will not infringe the rights of any third party;
 - 8.5.4** that the Contractor has not granted or assigned any rights of any nature in the Department's Intellectual Property Rights to any third party.
- 8.6** The Contractor shall ensure that any copyright materials produced by or on behalf of the Contractor shall be marked with the following copyright notice " © Crown Copyright 2021.

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

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

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

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

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

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

- 10.4.6 the Contractor is convicted (or being a company, any officers or representatives of the Contractor are convicted) of a criminal offence related to the business or professional conduct
- 10.4.7 the Contractor commits (or being a company, any officers or representatives of the Contractor commit) an act of grave misconduct in the course of the business;
- 10.4.8 the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil its obligations relating to the payment of Social Security contributions;
- 10.4.9 the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to fulfil its obligations relating to payment of taxes;
- 10.4.10 the Contractor fails (or being a company, any officers or representatives of the Contractor fail) to disclose any serious misrepresentation in supplying information required by the Department in or pursuant to this Contract.

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

11 Status of Contractor

- 11.1 In carrying out its obligations under this Contract the Contractor agrees that it will be acting as principal and not as the agent of the Department.
- 11.2 The Contractor shall not say or do anything that may lead any other person to believe that the Contractor is acting as the agent of the Department.

12 Confidentiality

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

- 12.1.1 treat the other party's Confidential Information as confidential and safeguard it accordingly; and
- 12.1.2 not disclose the other party's Confidential Information to any other person without the owner's prior written consent.

12.2 Clause 12 shall not apply to the extent that:

- 12.2.1 such disclosure is a requirement of Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA, Code of Practice on Access to Government Information or the Environmental Information Regulations pursuant to Clause 13 (Freedom of Information);
- 12.2.2 such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;
- 12.2.3 such information was obtained from a third party without obligation of confidentiality;
- 12.2.4 such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or
- 12.2.5 it is independently developed without access to the other party's Confidential Information.

12.3 The Contractor may only disclose the Department's Confidential Information to the Contractor Personnel who are directly involved in the provision of the 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 Amendment and variation

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

19 Assignment and Sub-contracting

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

20 The Contract (Rights of Third Parties) Act 1999

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

21 Waiver

No delay by or omission by either Party in exercising any right, power, privilege or remedy under this Contract shall operate to impair such right, power, privilege or remedy or be construed as a waiver

thereof. Any single or partial exercise of any such right, power, privilege or remedy shall not preclude any other or further exercise thereof or the exercise of any other right, power, privilege or remedy.

22 Notices

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

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

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

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

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

23 Dispute resolution

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

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

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

24 Discrimination

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

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

25 Law and Jurisdiction

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

As witness the hands of the parties

Signed by a person authorised to sign on behalf of **Virtual College Ltd**

Signature:	{{Sig_es_:signer1:signature}}
------------	-------------------------------

Name:	{{ N_es_:signer1:fullname}}
-------	-----------------------------

Role:	{{ Ttl_es_:signer1:title}}
-------	----------------------------

Date:	{{ Dte_es_:signer1:date}}
-------	---------------------------

Signed by person authorised to sign on behalf of the Secretary of State for Education:

Signature:	{{Sig2_es_:signer2:signature}}
------------	--------------------------------

Name:	{{ N2_es_:signer2:fullname}}
-------	------------------------------

Role:	{{ Ttl2_es_:signer2:title}}
-------	-----------------------------

Date:	{{ Dte2_es_:signer2:date}}
-------	----------------------------

Schedule 1: Services

1.1- Key Personnel

In accordance with clause 7.4, the individuals listed in the table below are Key Personnel:

Name	Role	Period of Involvement
[REDACTED]	DfE Contract Manager	Ongoing
[REDACTED]	DfE Team Leader, Children in Need Outcomes Unit	Ongoing
[REDACTED]	DfE Unit Leader, Children in Need Outcomes Unit	Ongoing
[REDACTED]	DfE Commercial advisor	Procurement and set up period
[REDACTED]	VC Account Manager	Ongoing
[REDACTED]	VC Contract Manager	Procurement and set up period
[REDACTED]	Learning Design & Project Manager	Ongoing
[REDACTED]	Senior Project Manager	Ongoing

1.2- Key Sub-Contractors

In accordance with clause 7, the Contractor may sub-contract its obligations under the Contract to the Sub-Contractors listed in the table below.

Key Sub-Contractor Name and Address (if not the same as the registered office)	Registered Office and Company Number	Related Product/Service Description	Sub-contract Price expressed as a percentage of total projected Charges over Term	Role in delivery of the Services
[REDACTED] Ashton House, 95 Priors Way, Bray, Maidenhead SL6 2EN.	N/A	Project management and consultancy services	7%	Strategic project management and subject matter expertise
<Redacted> Pearl Safeguarding Consultancy Muir, Camault Muir, Kiltarlity, Beaul, Highlands Scotland, IV4 7JH	N/A	Project management and user research services	18%	Operational project management, user research management and subject matter expertise
Various Subject Matter Experts - identified from a bank of quality assured subcontractors	N/A	Subject matter expertise	24%	Creating and curating content and providing expertise in sector/subject.

1.3- Project plan

The below project plan and risk register are subject to change and will be updated throughout the contract duration. An updated project plan will be agreed between both parties in line with the requirements of Section 1.5.

Task	Start	End	Cal. Days	Work Days
Discovery - User Research and Stakeholder engagement	25/10/2021	06/12/2021		
Project mobilisation and user research	25/10/2021	16/02/2022	115	83
Project Kick off	25/10/2021	26/10/2021	2	2
Review the scope of the project and the associated deliverables	25/10/2021	26/10/2021	2	2
Review overall development and delivery process and agree project and research methodology.	25/10/2021	26/10/2021	2	2
Initial Steering group meeting	27/10/2021	28/10/2021	2	2
Establish User group, define and agree research activities	29/10/2021	02/11/2021	5	3
Undertake research activities x 3 (concurrently) incl: surveys; online workshops; desktop review; smaller focus groups	03/11/2021	28/11/2021	26	18
Undertake secondary research activities	03/11/2021	18/11/2021	16	12
Data aggregation and analysis	29/11/2021	05/12/2021	7	5
Project methodology agreed. Initial research complete	06/12/2021	06/12/2021	1	1
Design - Content collection, analysis and solution design	01/11/2021	05/01/2022		
Content Collection and Authoring	01/11/2021	05/01/2022	66	48
Identification and curation of existing content/resources	01/11/2021	05/11/2021	5	5
Identification of relevant case studies, scenarios and examples	06/11/2021	10/11/2021	5	3
Identification of core content requirements	11/11/2021	15/11/2021	5	3
Content authoring	16/11/2021	08/12/2021	23	17
Content analysis	09/12/2021	13/12/2021	5	3
Produce content approach recommendations	14/12/2021	18/12/2021	5	4
Content approach and themes reviewed by User Group and Steering Group (extended review period due to Christmas)	19/12/2021	03/01/2022	16	11
Content approach and themes approved by User Group and Steering Group	04/01/2022	04/01/2022	1	1
Content sign off	05/01/2022	05/01/2022	1	1
Design - Digital design	04/12/2021	05/01/2022		
Design standards and technical specification	04/12/2021	05/01/2022	33	23
Produce outline design standards and creative approach, including design style, accessibility, language and brand values	04/12/2021	08/12/2021	5	3
Produce rapid prototype, including all of the core design elements and standards, to create a blueprint for future development	09/12/2021	18/12/2021	10	7

Design Standards reviewed by User Group and Steering Group (extended review period due to Christmas)	19/12/2021	03/01/2022	16	11
Design Standards approved by User Group and Steering Group	04/01/2022	04/01/2022	1	1
Design Standards sign off	05/01/2022	05/01/2022	1	1

Resource Development - Sprint 1 (2 themes - 20 x assets)	10/01/2022	01/03/2022	51	37
Beta build - using agreed Content and Design Standards	10/01/2022	10/01/2022	1	1
Technical build - Beta build Sprint 1	11/01/2022	31/01/2022	21	15
Beta version reviewed by User Group and Steering Group	01/02/2022	07/02/2022	7	5
Beta version approved by User Group and Steering Group	08/02/2022	08/02/2022	1	1
Gold / Final build - implementation of Beta Feedback	09/02/2022	09/02/2022	1	1
Technical build - Gold / Final build Sprint 1	10/02/2022	23/02/2022	14	10
Gold version reviewed by User Group and Steering Group	24/02/2022	26/02/2022	3	2
Gold version approved by User Group and Steering Group	27/02/2022	28/02/2022	2	1
Approve final build - Sprint 1	01/03/2022	01/03/2022	1	1
Resource Development - Sprint 2 (2 themes - 20 x assets)	24/01/2022	15/03/2022	51	37
Beta build - using agreed Content and Design Standards	24/01/2022	24/01/2022	1	1
Technical build - Beta build Sprint 2	25/01/2022	14/02/2022	21	15
Beta version reviewed by User Group and Steering Group	15/02/2022	21/02/2022	7	5
Beta version approved by User Group and Steering Group	22/02/2022	22/02/2022	1	1
Gold / Final build - implementation of Beta Feedback	23/02/2022	23/02/2022	1	1
Technical build - Gold / Final build Sprint 2	24/02/2022	09/03/2022	14	10
Gold version reviewed by User Group and Steering Group	10/03/2022	12/03/2022	3	2
Gold version approved by User Group and Steering Group	13/03/2022	14/03/2022	2	1
Approve final build - Sprint 2	15/03/2022	15/03/2022	1	1
Resource Development - Sprint 3 (2 themes - 20 x assets)	31/01/2022	22/03/2022	51	37
Beta build - using agreed Content and Design Standards	31/01/2022	31/01/2022	1	1
Deliver Beta build Sprint 3	01/02/2022	21/02/2022	21	15
Beta version reviewed by User Group and Steering Group	22/02/2022	28/02/2022	7	5
Beta version approved by User Group and Steering Group	01/03/2022	01/03/2022	1	1
Gold / Final build - implementation of Beta Feedback	02/03/2022	02/03/2022	1	1
Deliver Gold / Final build Sprint 3	03/03/2022	16/03/2022	14	10
Gold version reviewed by User Group and Steering Group	17/03/2022	19/03/2022	3	2
Gold version approved by User Group and Steering Group	20/03/2022	21/03/2022	2	1
Approve final build - Spring 3	22/03/2022	22/03/2022	1	1
Steering Group Meetings			6	0
Project initiation	27/10/2021	27/10/2021	1	1
Month 1 - November	22/11/2021	22/11/2021	1	1
Month 2 - December	20/12/2021	20/12/2021	1	1
Month 3 - January	17/01/2022	17/01/2022	1	1
Month 4 - February	21/02/2022	21/02/2022	1	1

Month 5 - March	21/03/2022	21/03/2022	1	1
Customer testing	22/03/2022	26/03/2022	5	4
Technical transfer of assets to DfE	22/03/2022	22/03/2022	1	1
DfE Upload of assets into .gov site and testing	23/03/2022	25/03/2022	3	3
Product launch	26/03/2022	26/03/2022	1	0

1.4- Risk register

Author	Date registered	Category	Cause	Event	Effect	Probability (P)	Impact (I)	Rating (P x I)	Risk Rating	Risk Response	Risk Status	Risk Owner
MA	17/09/2021	Projects	Stakeholder involvement	The number of stakeholders involved in the approval processes may cause delays in scheduled feedback	Negative impact on the timings schedule potentially causing delays to delivery	2	3	6	Moderate	Development process to include adequate review periods and advance communication of any changes or delays. Protocols of review/feedback agreed with DfE and stakeholders at start of project.	Ongoing	VC
MA	17/09/2021	Tech	Inadequate consideration given to the way the assets will appear on the web page and that they are compatible	Last minute changes end up being necessary, causing delays to the project	Negative impact on the timings schedule potentially causing delays to delivery	1	2	2	Low	Testing of prototype and development of learner journey will mitigate this risk	Ongoing	VC
MA	17/09/2021	Projects	Conflicting feedback from DfE stakeholders likely to cause delays due to additional time required to obtain clarity of requests	Would result in additional times required to implement feedback and changes	Negative impact on the timings schedule potentially causing delays to delivery	2	3	6	Moderate	DfE to nominate a moderator who will review feedback before presenting to VC. Support from VC provided if required, on effective ways of managing this. VC to set up a core group with a lead SME to manage conflicting feedback.	Ongoing	DfE/VC
MA	17/09/2021	Projects	Number of assets and scope of assets falls outside of proposal and quotation	More assets required with higher levels of complexity	An impact on timings and costs	2	4	8	Moderate	Completing a robust research phase with priorities agreed with user group and DfE steering group approval	Ongoing	VC

DM	21/09/2021	Projects	Project Kick off meeting delays	Delays in contract award or kick off meeting arrangements may cause delay to whole project, depending on extent.	Negative impact on remainder of project, reducing time for research, feedback, development or overall delivery	1	2	3	Low			
DM	21/09/2021	Projects	User research group difficult to engage	Further lockdowns, high sickness/absence rates or additional work commitments may reduce number of users willing to participate in research	Negative impact on validity of research, informing findings, testing and subsequent development of resources might not be fully reflective or accurate.	2	3	6	Moderate			
DM	21/09/2021	Projects	Additional themes identified	A significant number of additional themes and related resources required based on user research	Impact on capacity of user groups to gain feedback and test due to volume of involvement. Impact on project timescale to design and develop resources with contractual arrangement	1	3	3	Low			

1.5- The Service Specification

Overview

To support Designated Safeguarding Leads (DSLs) with the complexities and challenges of their role, the DfE is looking to procure a Contractor to develop a set of online resources to support DSLs. Further details are set out in the 'Detailed Requirements' section.

The resources will also need to address how DSLs can promote the educational outcomes of children who have or have had a social worker and the type of additional support children with a social worker need. This includes improving the visibility of this group and supporting staff to improve their engagement with learning. These changes to the DSL role are grounded in the findings of the Children in Need Review.

The toolkit will be hosted on existing DfE content pages on .GOV.UK. It will reflect the information provided in Annex C: Role of the Designated Safeguarding Lead of the Keeping Children Safe in Education (KCSIE) statutory guidance. The resources are intended to complement rather than replace existing training and support that DSLs already receive.

Suppliers will be expected to have expertise in child protection and safeguarding as well as established links with DSLs, education settings, including both schools and colleges, and children's social care.

Background

KCSIE sets out that all schools and colleges should have a DSL. The DSL has lead responsibility for safeguarding and protecting all children in their school or college. They also play a critical role in the lives of children who have or have had a social worker, by safeguarding them, and by supporting their wider welfare, including promoting their educational outcomes.

The role of the DSL carries a significant level of responsibility. KCSIE sets out that the DSL should be a senior member of the school or college's senior leadership team.

These responsibilities are set out in more detail within 'Annex C: Role of the designated safeguarding lead' of KCSIE. However, in summary the role includes:

- providing advice and support to other staff on child welfare, safeguarding and child protection matters;
- taking part in strategy discussions and other inter-agency meetings, and or supporting other staff to do so; and
- managing referrals to LA social services, the police, and other agencies such as the Disclosure and Barring Service and, or the Teacher Regulation Agency.

The DSL is also expected to:

- promote educational outcomes by knowing the welfare, safeguarding and child protection issues that children in need are experiencing, or have experienced, and identifying the impact that these issues might be having on children's attendance, engagement and achievement at school or college.
- act as a point of contact with the safeguarding partners i.e. the local authority; a clinical commissioning group for an area within the local authority; and the chief officer of police for an area any part of which falls within the local authority area.
- liaise with the headteacher or principal to inform him or her of issues (especially ongoing enquiries under section 47 of the Children Act 1989 and police investigations).
- promote supportive engagement with parents and/or carers in safeguarding and promoting the welfare of children, including where families may be facing challenging circumstances.

DSLs are expected to undergo training to provide them with the knowledge and skills required to carry out their role effectively. This training should be updated at least every two years and their knowledge and skills should be refreshed regularly via e-bulletins, meeting other DSLs, and taking time to read and digest safeguarding developments at regular intervals, as required, and at least annually, to allow them to understand and keep up with any developments relevant to their role.

Detailed requirements (THE SERVICES)

The Contractor's role will be to:

- Create online resources/ materials, which meet policy objectives and the diverse needs of users, in order to give appropriate support to DSLs.

The Indicative Content for the online resource is set out on pages 3-5 below. This list outlines the expected set of practice areas that the online resource will cover however this list may be added to in the early stages of the project, following further user engagement. The Contractor will need to demonstrate flexibility in responding to additional user needs.

Indicative Content for DSL Online Resource:

Resources will need to:

- align with and reference Keeping Children Safe in Education, Working Together to Safeguard Children, Relationships and Sex Education and Health Education statutory guidance as well as other relevant statutory guidance and legislation;
- reflect relevant content detailed in the RSHE teacher training modules on .GOV.UK Teaching about relationships, sex and health - GOV.UK (www.gov.uk);
- meet the diverse needs of DSLs and wider school and college staff; and
- address the diverse needs of children and young people in relation to safeguarding and child protection. In particular, resources will need to support DSLs to respond to the particular safeguarding risks and barriers that children with SEND, mental health issues and different protected characteristics may experience.

Theme	Detail	Types of content to include
<p>Specific forms of abuse and safeguarding issues including:</p> <ul style="list-style-type: none"> • Child criminal exploitation • Domestic abuse • Emotional abuse • Homelessness • 'Honour' based abuse including FGM and forced marriage • Issues relating to witchcraft, religion and implications for the effective safeguarding of children • Missing from home or education • Modern slavery and trafficking • Neglect • Online abuse/harassment • Parental mental health • Physical abuse • Radicalisation and extremism • Serious violence/knife crime • Sexual harassment in public places • Stalking • Substance abuse (drug and alcohol) – child and parental <p>Resources on child sexual abuse will be included in the online resource for DSLs however these will be developed</p>	<ul style="list-style-type: none"> • Definition of different types of abuse or safeguarding issues • Signs/indicators of different types of abuse or safeguarding issues • Working with parents/carers • Communicating with children and young people with diverse needs • Whole school/college approaches to preventing abuse/identifying abuse/encourage reporting of abuse/responding to reports of abuse and supporting victims and perpetrators of abuse. 	<ul style="list-style-type: none"> • Links to relevant statutory guidance and legislation • Key messages from research • Resources for DSLs and staff e.g. handouts and toolkits • Good practice case studies • List of relevant webpages for further information

separately. These resources will include information on: <ul style="list-style-type: none"> • Harmful sexual behaviours; • Peer-on-peer abuse; • Child sexual exploitation. 		
Barriers to children and young people reporting concerns to staff and the DSL	<ul style="list-style-type: none"> • Speaking to children and young people with diverse needs about concerns • Common barriers to reporting concerns • Strategies for overcoming this 	<ul style="list-style-type: none"> • Links to relevant statutory guidance and legislation • Key messages from research • Resources for DSLs and staff • Good practice case studies • List of relevant webpages for further information
Barriers to staff reporting concerns about children and young people	<ul style="list-style-type: none"> • Common barriers to reporting concerns • Strategies for overcoming this 	<ul style="list-style-type: none"> • Links to relevant statutory guidance and legislation • Key messages from research • Resources for DSLs and staff • Good practice/examples on reporting concerns and drafting effective reports/referrals • List of relevant webpages for further information
Allegations made against/concerns raised in relation to teachers	<ul style="list-style-type: none"> • Understanding allegations that meet the harms threshold and the role of the LADO • Understanding what a low-level concern is and having effective mechanisms to report these 	<ul style="list-style-type: none"> • Links to relevant statutory guidance and legislation • Resources for DSLs and staff • Good practice case studies • List of relevant webpages for further information
Working effectively with safeguarding partners	<ul style="list-style-type: none"> • Understanding the role of different safeguarding partners • Strategies for effective engagement 	<ul style="list-style-type: none"> • Links to relevant statutory guidance and legislation • Resources for DSLs and staff • Key messages from research • Good practice case studies • List of relevant webpages for further information

Promoting the educational outcomes of children with a social worker	<ul style="list-style-type: none"> • Understanding the impact that issues such as adversity and trauma can have on children who have or have had a social worker • Common issues that children with a social worker may be experiencing at home • Communicating the needs of children with a social worker to school and college staff, and ensuring that they are visible • Promoting high aspirations for children with a social worker • Supporting children with a social worker to reach their potential 	<ul style="list-style-type: none"> • Links to relevant statutory guidance and legislation • Key messages from research including the Children in Need Review • Resources for DSLs and staff • Good practice case studies • List of relevant webpages for further information
---	--	---

Proposal:

- Establish a user research group of DSLs, headteachers/principals and other relevant child welfare/safeguarding professionals who will be involved in co-producing and testing prototypes of the resource; develop a user research plan;
- Develop resources in partnership with users, subject-matter experts, policy officials and the DSL Online Resource steering group (to be established) which are iterated following user testing and stakeholder engagement;
- Identify existing research and good practice examples including from relevant Government publications, e.g. the Children in Need Review, and translate them into user-friendly resources;
- Develop a quality assurance process for good practice examples/case studies, working with the Department and the steering group;
- Design resources that achieve WCAG 2.1 level AA standards as part of meeting the government accessibility requirements;
- Work with the Department's policy and digital teams to structure the content in a way that ensures users can find what they need easily and give them a good user experience.

Administration

- Production of a detailed project delivery plan for the length of the contract, by 14th January 2022.
- Production of a high level asset register by 14th January 2022. Any changes will be revised via a change control note.
- Production of an Exit Plan to be prepared by the end of January 2021 outlining how the service will be wound down.

Reporting and information

- Attend weekly meetings with the DfE project manager to monitor and review progress;
- Monthly Show & Tells to share key findings from user research/testing and progress on content development; frequency may increase to fortnightly for final months of project (January-March);
- Provide monthly reports on progress against KPIs;

- Support DfE to respond in a timely manner to relevant correspondence or parliamentary questions related to the project on an ad-hoc basis.

Key Performance Indicators (KPIs)

The contractor will be expected to develop a set of online resources, in line with the indicative content on pages 22-25 of the Service Specification.

- The final set of resources produced will need to be approved by:
 - The user group, established by the Contractor;
 - The DSL Online Resource steering group, established by the DfE, and comprising subject experts, policy officials and relevant practitioners;
 - The DfE digital team.

Final approval will rest with the DfE contract management team.

The table below sets out in more detail the key KPIs for the duration of the project:

KPI	Measurement Period	Performance Measure	Service Period (8 months, December 2021 to July 2022)	Monitoring method
Satisfaction of steering group with the resources developed	Monthly	90%	Ongoing until 31 July 2022	Monthly contract meeting
Satisfaction of user research group with the resources developed	Monthly	90%	Ongoing until 31 July 2022	Monthly contract meeting
Presentations for Show & Tells and steering group meetings shared 3 business days in advance	Monthly	90%	Ongoing until 31 July 2022	Monthly contract meeting
Monthly progress reports received by DfE within a week of month ending	Monthly	100%	Ongoing until 31 July 2022	Monthly contract meeting
Production of a delivery plan for the length of the contract, within 2 weeks of contract start date	Monthly	100%	Ongoing until 14 January 2022	In 1 st monthly contract meeting
Agreed delivery milestones achieved within 5 working days of original date	Monthly	100%	Ongoing until 31 July 2022	Monthly contract meeting

The Contractor will produce a short, monthly report on progress against KPIs.

Project timescales

The work will begin in mid- December 2021 and be completed by end of June 2022. The below table sets out timescales for key activity:

December 2021	<ul style="list-style-type: none"> Contract finalised and signed Collaboration on steering group plans with DfE
January 2022	<ul style="list-style-type: none"> Stakeholder plan developed Risk and issue log developed User research plan developed Project plan developed First meeting with steering group User research group established and user research started
February 2022	<ul style="list-style-type: none"> Monthly meeting with steering group Existing resources identified, compiled and where appropriate, updated for DSL audience. Gaps in resources/content identified
March 2022	<ul style="list-style-type: none"> Monthly meeting with steering group Existing resources formatted to align with tech requirements (TBC) Case studies identified New content writing commenced (as per specification and agreed list with DfE from first steering group)
April 2022	<ul style="list-style-type: none"> New content drafted to meet gaps and circulated to steering group and user group for review and feedback Ongoing user testing
May 2022	<ul style="list-style-type: none"> Resources re-drafted following testing
June 2022	<ul style="list-style-type: none"> Resources signed-off .GOV.UK page designed with DfE content designers Online resource launched

Mandatory and desirable skills and requirements (THE BIDDER)

The successful Contractor must demonstrate the following mandatory requirements:

- Good knowledge and understanding of the role of the DSL, school and college safeguarding, children's social care and the educational outcomes of children with a social worker.
- Good knowledge and understanding of the diverse needs of children and young people in relation to safeguarding and child protection and the impact that SEND, mental health issues and different protected characteristics may have on this.
- Expertise in child protection and safeguarding including links with relevant subject-matter experts. This expertise should cover the issues outlined in the Indicative Content section (p.3-5).
- Established links with DSLs as well as education settings, including both schools and colleges, and children's social care stakeholders.
- Experience of shaping guidance and resources that help support safeguarding and promote educational outcomes, especially for vulnerable groups including children who have or have had a social worker.
- The skills and experience to work with the diversity of users of government services and to involve them in appropriate research activities.
- The skills and experience to develop high-quality resources - creating, updating and reviewing content that meets user needs, making information and guidance clear and easy for users to understand.
- The skills to carry out user research activity including behavioural insights and turn user research data into clear findings that inform decisions.
- The skills to implement user-centred design practices and embed them into an agile workflow to deliver timely findings.

- The skills to design user-focused services and a consistent, end-to-end user experience.
- The skills to work with Government digital platforms and comply with Government accessibility requirements.
- A highly organised and efficient approach to project management, with the skills to deliver outputs on budget and to challenging timescales.
- A good understanding of the objectives of the Public Sector Equality Duty, under s149 of the Equality Act 2010, and its relevance to the role of the DSL. The Contractor will need to work with the Department to ensure that these objectives are considered and implemented in the development of the resources.
- A good general understanding of data handling in the context of Data Protection legislation and its relevance to the role of the DSL.

The following requirements are considered desirable:

- good understanding of Departmental strategy and objectives.
- experience of delivering a government project that has been built in accordance with GDS guidelines to deliver digital content for .GOV.UK and/or a digital service.

We would expect the service team to include: subject and policy expert(s), user researcher(s), a project manager and content designer(s). The content designer(s) will be supported by content design resource within DfE who will be responsible for the .GOV.UK page content and format decisions. The service team will work closely with DfE policy and digital colleagues throughout the duration of the project.

The Contractor's solution

1. Policy solution

With reference to Document 3 (Service Specification) and guidance below, please set out how you will deliver the required policy solution.

Requirement:

The bidder should set out:

- a) Their existing connections to Designated Safeguarding Leads (DSLs) in schools and colleges and relevant education and children's social care professionals and how they would quickly establish a diverse user group to test and develop the materials for the online resource with.
- b) Their knowledge and understanding of the role of the DSL in schools and colleges; the key challenges that DSLs experience and how their solution can help address those challenges.
- c) Their expertise in child protection and safeguarding including links with relevant subject-matter experts; and their skills and expertise to deliver the Indicative Content set out in the Service Specification.
- d) Their knowledge and understanding of the role of DSLs in promoting the educational outcomes of children with a social worker and how their proposed solution would support DSLs with this aspect of their role.
- e) What barriers and challenges they envisage in developing the online resources for DSLs and how they would overcome those challenges.

Supplier response:

Word Count = 850

- a) Over the last two decades, Virtual College has worked with experts from multidisciplinary safeguarding training backgrounds to create practical and accessible online resources for the public sector.

Our team for this project has established links to DSLs, covering the spectrum of education (primary, secondary, 16+ education, SEN), as well as children's social care:

- [REDACTED] - Programme Director with 20+ years in the education sector
- [REDACTED] - Project Lead - managing research, recommendations and acting as core subject matter expert (SME)
- SMEs across the education sector to author content, which will be peer reviewed and approved by our specialist team members.

Team members:

- Virtual College - developed [online safeguarding resources](#) to over two million public sector employees. Expertise in managing SMEs from different organisations and backgrounds, bringing together stakeholders and users across multiple agencies (police, healthcare, social care and education) to create multi-agency safeguarding training
- Education Safeguarding Programme Director and Project Lead - specialists with well-established links to DSL's and school leaders
- The Education & Training Foundation (ETF) – strategic workforce development representing FE, independent and specialist colleges
- National Association of Managers of Student Services – 300 member organisations, 95% are FE colleges

- Operation Encompass - police and education safeguarding partnership with 6700 trained users in education
- Annemarie Millar - Children's Rights Consultant and Trainer

Our aim for this project is to ensure the voice of the child/student is at the centre of the resources.

With access to nationwide DSLs via our digital learning database, and through our network links, we have a user group plan, research practitioners in place, and the technology ready to engage a group.

We will seek diverse representation from DSLs in different settings and regions. The group will be used to share feedback, shape content (following DfE themes), co-create and test prototypes.

Our plan includes using ETF's survey conducted to 600+ DSLs, for up-to-date recommendations on training requirements.

We appreciate resources need to complement, rather than replace, existing training and guidance. The research phase will identify and curate existing resources to avoid duplication.

b) Our team knows from first-hand experience within the education sector that some of the core challenges DSLs face are:

- format/access of materials
- balancing speed, accuracy and nature of responses
- information/challenges relevant to their setting
- staying in-the-know with local and national guidance/legislation

We also know that DSLs want to:

- prioritise their duties/workload better
- create a culture of listening within their schools/colleges
- build positive relationships with safeguarding partners
- support parents/carers and the wider community
- share best practice within a supportive DSL community

Keeping in mind the 'voice of the child/student', we will create a toolkit of just-in-time resources that offer practical, simple, easily accessible materials that support DSLs to take relevant action.

To achieve project goals, our specialist group of SMEs will author content to meet DSL/DfE objectives. This will include creation of circa 60 online assets (subject to approval from user group and DfE).

Given the reality of the DSL role, we recommend linking to a helpline service within the resources ([Operation Encompass National Helpline](#)), staffed by Educational/Clinical Psychologists to provide support to staff in education settings with children experiencing domestic abuse.

c) Through us, the DfE will be working with a team with vast experience of 'life' as a DSL, as well as a digital learning organisation bringing extensive expertise to design and develop the Indicative Content.

Our team's experience includes shaping resources, policies and training materials, and interpreting national guidance for DSLs to embed in school/college policies.

Evidence of work:

- [ETF](#)
- [NAMSS](#)
- [Annemarie Millar](#)

From an online resource perspective, Virtual College has delivered online safeguarding training since 2006. The content we produce adheres to WCAG 2.1 level AA standards.

Virtual College worked with Sutton SCB on their findings from a high-profile Serious Case Review. Managing a diverse group of multi-agency SME's (education, health, police, social care), we identified 10 key learning principles. The core group provided feedback and collaborated across the wider stakeholders and had ultimate sign-off on the direction and the content.

[The resulting toolkit](#) reflected the themes and challenges faced by safeguarding professionals in their day-to-day roles.

d) We recognise that there may be a different strategic lead for promoting the educational outcomes of children who have, or have had, a social worker.

In this case, the DSL must work closely with the lead to provide strategic oversight for the outcomes of these children/young people

Our team has in-depth knowledge of the day-to-day roles and responsibilities of DSLs in promoting the educational outcomes of children with a social worker, and are currently working on an offer of support involving FAQ's and website to signpost services/guidance.

We will also engage with The Virtual School to include those who provide strategic oversight for the improvement of outcomes for such children / young people.

Our solution will support DSLs specifically through including downloadable 'best-practice' guides and just-in-time aids, FAQ's including signposting, to cover the types of additional support required.

Online assets will be tailored to suit varying DSL needs, including relevant information for professionals, young people, parents/carers, and DSLs supporting children with a social worker. Differentiated content will reflect needs of different groups (Primary/Secondary/FE/College/SEND).

e) We envisage the following challenges:

- tailoring content to cover every level/age group of the DSL role
- ensuring everyone is heard and feedback is representative
- content remains reflective of national/local guidance
- capacity of DSLs to commit to research/feedback process
- managing a large group of stakeholders with differing views through to a synced solution that meets all requirements

To overcome challenges, we have:

- contractual agreements which ensure commitment for the duration of the contract
- acceptable incentives for DSLs (subject to DfE approval)
- online software to collate DSL feedback and track trends
- a focus group of SMEs to define the final recommendations for materials, subject to DfE approval.

Our expertise lies in our ability to:

- Work with multiple stakeholders/SMEs
- Focus on the user and their level of engagement to encourage real behaviour change
- Build trusted relationships quickly
- Be flexible and pragmatic
- Deliver to time, quality and budget
- Deliver sustainable resources

2. User research and digital skills

With reference to Document 3 (Service Specification) and guidance below, please set out how you will meet the required user research and digital skill requirements.

Requirement:

The bidder should set out their skills and experience in:

- a) Producing high-quality resources - creating, updating and reviewing content that meets user needs, designing and making information and guidance clear and easy for users to understand.
- b) Identifying and working with the diversity of users of government services and involving them in appropriate research activities.
- c) Planning and carrying out user research activity including behavioural insights and turning user research data into clear findings that inform decisions.
- d) Implementing user-centred design practices and embedding them into an agile workflow to deliver timely findings.
- e) Designing a consistent, joined-up, end-to-end user experience.
- f) The skills to work with Government digital platforms and comply with Government accessibility requirements.

3. Project and risk management

With reference to Document 3 (Service Specification) and guidance below, please set out how you will fulfil the project and risk management requirements.

Requirement:

The bidder should set out:

- a) A high-level project plan, outlining key activities, timescales, milestones and allotted resources. This should include how and when they would engage users. Bidders must attach a project plan as a separate annex that will not count towards the word limit (max. 1 page).
- b) Identify the specific risks and issues that you foresee in delivering this project and set out what contingencies and countermeasures would be put in place to mitigate the risks. Bidders should also attach a risk register as a separate annex that will not count towards the word limit (max. 1 page).
- c) Their skills to deliver outputs on budget and to challenging timescales.

Supplier response:

Word Count = 454 words

- a) Please see the Project Plan attached.
- b) Please see the Risk Register attached.

Potential Risks	Contingencies and Countermeasures
Capacity of DSLs to continue to engage with research	Incentives
Resources being accessible to all users	Creating resources fit for purpose that reflect the specific needs of users at varying levels
Resources being kept up-to-date and accurate to reflect local/national picture	Consider having a member of the team on retainer to ensure that updates can be maintained regularly and effectively to reflect legislative changes
Accurate and effective feedback to reflect user	Use methods that allow DSLs to respond with minimal time and effort involved but that will

group needs due to time constraints	reflect the needs they face including engagement in twilight sessions
-------------------------------------	---

c) Virtual College works with around 50,000 organisations every year.

With a team of 100+ employees, we have capacity to manage projects at the highest level.

When a new project has been agreed, we assign a dedicated team with specific roles and responsibilities. As well as project managing each stage as it is live, we monitor against overall objectives to ensure services are delivered on time, to budget and goals.

One of the best demonstrations of our capability to deliver at pace to tight deadlines and meet extensive KPIs, is the £80 million training programme we led with the Ministry of Defence (MoD). This was the transformation of face-to-face resources to the very latest technology enhanced learning methods.

Virtual College worked closely with the UK MoD over a 5-year period, which began with creating a unique learning strategy and setting out a blueprint for course design, development and deployment.

We undertook a series of facilitated sessions, using a mixed approach of 1:1s, group sessions and site visits across the United Kingdom, to establish and agree:

- user needs/requirements
- project aims, objectives, outputs and outcomes, process, approach and timelines
- reporting/governance
- measures of success
- style, brand, look and feel of digital resources
- evaluation and impact measurement

Virtual College was required to be highly flexible in its approach, providing innovative leading-edge solutions in an agile way, which adapted to evolving and rapidly changing priorities.

A training needs analysis (TNA) was conducted through collaboration with key personnel and a steering group was formed to manage the entire process.

A comprehensive TNA report was written following an extensive information gathering exercise (analysing existing documentation and interviewing stakeholders). This was overlaid with the training vision to create a map identifying capability and skills gaps in a final written scoping study.

We presented this back to key stakeholders to ensure the mapping was accurate and truly reflected the current situation and the training vision for the future.

Virtual College's flexible partnership approach to managing this programme has been essential to its success. This was based around establishing a 'one team' working ethos with the client as opposed to a purely contractual relationship.

4. Social Value

The social value model, as outlined in [Procurement Policy Note 06/21](#)¹, will be applied to all new procurements from 1 January 2021. Social value has a lasting impact on individuals, communities and the environment.

For this contract we are interested in how bidders will support the outcome of **Improve community integration**.

Please set out how you will fulfil the Social Value requirements.

Requirement:

The bidder should set out:

- a) When answering this question, please include: Your 'Method Statement', stating:
- How you will collaborate with users and communities in the co-design and delivery of the contract to support strong integrated communities.
 - Influence staff, suppliers, customers and communities through the delivery of the contract to support strong, integrated communities.
 - Your committed number of people-hours spent supporting local community integration, such as volunteering and other community-led initiatives, under the contract.

Supplier response:

Word Count = 397

a) We will:

- Work with experienced partners with established links to relevant users and communities to source real, lived experience and feedback
- Develop a set of standards for the user group – respect others' feedback; all have an equal voice, confidentiality
- Share a system of online research methods with users for ease of access
- Share contact details (with permission) for community support
- Set-up focus groups - offering signposted support for parents/carers

b) We will:

- Ensure all communications are via an experienced and qualified SME who provides accurate, up-to-date information
- Identify points of challenge/barriers or training needs of users during the process, communicating with individual DSLs to discuss and offer support (through our SMEs) and signposting to relevant resources
- Reach out to unsuccessful bidders (with approval from DfE) to ask for their involvement in this project, recognising their expertise and commitment to the sector
- Signpost DSLs to other sources / suppliers of support as part of the toolkit -, NSPCC, Contextual Safeguarding Network
- Create an understanding in the toolkit around extra familiar harm. Building on how we influence system change across wider communities, who play a part in creating safe cultures by reporting risky behaviours, sharing local intelligence to help disrupt criminal activity and upskill businesses, parents and local communities to recognise risk and seek help early.
- Reflect a whole workforce approach in the toolkit, sharing best-practice and clear guidance on working in a trauma informed way to address culturally embedded issues and stigma to break down barriers and unconscious bias to ensure best

¹ <https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts>

outcomes for children and young people at every stage.

c)

- Provide 4 x 1 hour webinars (over 1 year), facilitated by safeguarding SMEs, as a safe opportunity for DSLs to share experience and support (+ 6 hours follow-up including signposting and support)
Total = 10 hours
- Operation Encompass Teachers' National Helpline – free advice from an Education Psychologist on how to support a child in school who is experiencing domestic abuse
- Online key adult training from Operation Encompass - free training aimed at education settings
- Free access to online courses/resources including:
 - [Keep Them Safe: Protecting Children from Child Sexual Exploitation](#)
 - Mental Health and Wellbeing
 - Resilience
 - Personal Development
 - Dealing with Stressful Situations
 - Listening

6 hours of learning – unlimited access for users
- Provide a designed poster/infographic to promote the toolkit and additional resources. Emailed out to all stakeholders / users for local distribution. Inhouse design and marketing time = 8 hours.

5. Cost and Value for Money

With reference to Document 3 (Service Specification) and guidance below, please set out how you will fulfil the project and risk management requirements. Potential Suppliers must complete all relevant tabs of the Cost Matrix (Document 6), providing a full breakdown and justification of the costs you detail. The Department reserves the right not to consider a bid that does not include a fully completed cost matrix.

Requirement:

The bidder should set out:

- a) Clear, detailed costings for each element, demonstrate that your proposed charges are based on efficient models of delivery and provide good value for public money.
- b) You must ensure that all estimated costs are real, auditable and can be justified. Be sure you separately identify and include all expenditure that you expect to incur in relation to proposed activities, i.e. costs associated with overheads e.g. premises/facilities/licences and staffing, e.g. management, delivery and administration.

Up to 5 marks are available for the detailing of cost assumptions. The bidder should set out in the Cost Matrix:

- The assumptions made in terms of costs e.g. number of days/FTE allocated per staff.
- How they have ensured the budget is sufficient for the work required.

Please set out how you have ensured the budget is sufficient for the work required.

- We're offering a fixed price based on specification and time
- We've analysed the work required, have undertaken preliminary engagement activities with our network partners (programme director and project lead) to identify and agree the appropriate and realistic timeframes to undertake the work required, particularly around the research, review and feedback cycles
- Days allocated to staff roles are calculated on this analysis, experience and discussions with the individual partners, programme director and project lead
- Includes the interaction and communication with the DfE steering group for approval and sign off, based on working with government departments on similar projects
- We have taken into consideration our previous experience and data in delivering similar scale and scope of projects in the past and used our legacy data and experience in evaluating the effort required.
- We will ensure that we monitor this budget closely to avoid any overspend by:
 - Completing Research and Design to ensure that we understand exactly how to create online resources that offer best value for money
 - Monitoring costs closely through a robust project management approach
- Our development process is based on creating approx. 60 assets (output pdf and ppt), applying our average development timings/days based on experience of creating similar resources
- Our development process includes a process and software for user and stakeholder feedback and review, with scheduled timings throughout the contract to ensure that the product we create meets user needs. Based on previous experience of managing complex stakeholder engagement and feedback.
- Testing of the products is included both from a user perspective and also for the digital hosting.
- Assumptions are based on specification and timescales stated are subject to scoping

Schedule 2

Payment information

1. Payments will be made monthly in arrears. The first monthly payment will be made at the end of the month following the first month of the contract.



Invoicing schedule:

31/01/2022: £34,983
28/02/2022: £34,983
31/03/2022: £34,983
30/04/2022: £34,983
31/05/2022: £34,982
30/06/2022: £34,982

- 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 monthly in arrears and shall be detailed against the expenditure headings set out in the Table. 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 30 days of the end of the month electronically by email to accountspayable.OCR@education.gov.uk, quoting the Contract reference number. To request a statement, please email accountspayable.BC@education.gov.uk, 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

Schedule 3

Schedule 3a

Processing, Personal Data and Data Subjects

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

1. The contact details of the Controller's Data Protection Officer are: [REDACTED] Department for Education.
2. The contact details of the Processor's Data Protection Officer are: [REDACTED], Quality & Compliance Manager email: <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	<p>The personal data that will need to be processed as part of the contract is:</p> <ul style="list-style-type: none">• Names of members of the steering group• Email addresses of members of the steering group <p>The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.</p>
Duration of the processing	The duration of the processing is from 15 December 2021 until 31 July 2022.
Nature and purposes of the processing	<p>The nature of processing includes collection, recording, storage and use.</p> <p>The purpose is stakeholder engagement.</p>

Type of Personal Data	Names Email addresses
Categories of Data Subject	Members of the public
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	The data will be destroyed by the Contractor within one month of the contract end date.

Schedule 3b

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

1.1 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).)

1.2 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, namely that contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials 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.)

- 1.3 Where clause 1.2 of this Schedule 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.)

- 1.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle 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).
- 1.5 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 1.14 of this Schedule.
- 1.6 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.
- 1.7 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.
- 1.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:
- physical security controls;
 - good industry standard policies and processes;
 - malware protection;
 - boundary access controls including firewalls, application gateways, etc;
 - maintenance and use of fully supported software packages in accordance with vendor recommendations;
 - use of secure device configuration and builds;
 - software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
 - user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
 - any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
 - retained and protected from tampering for a minimum period of six months;
 - made available to the department on request.
- 1.9 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.
- 1.10 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.

1.11 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>.

1.12 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".

1.13 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.

1.14 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 1.15 of this Schedule.

- 1.15 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.

- 1.16 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.
- 1.17 All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.
- 1.18 The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 1.19 Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, 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.

- 1.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using 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.
- 1.21 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.
- 1.22 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.
- 1.23 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.
- 1.24 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.
- 1.25 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.