Department for Education

CONTRACT FOR ASSESSING THE ONLINE LEARNING LANDSCAPE FOR UPSKILLING AND RESKILLING ADULTS: THE CURRENT MARKET AND THE USE OF ARTIFICIAL INTELLIGENCE

PROJECT REFERENCE NO: DFERPPU/2018/029

This Contract is dated

Parties

1) The Secretary of State for Education whose Head Office is at Sanctuary Buildings, Great Smith Street, LONDON, SWI P 3BT ('the Department"); and
2) ICF Consulting Services Ltd whose registered office is [redacted] ('the Contractor').

Recitals

The Contractor has agreed to undertake the Project on the terms and conditions set out in this Contract. The Department's reference number for this Contract is DFERPPU/2018/029.

Commencement and Continuation

The Contractor shall commence the Project on the date the Contract was signed by the Department (as above) and, subject to Schedule Three, Clause 10.1 shall complete the Project on or before 28/09/18

Contents

Signatories page 39

1.Interpretation

1.1 In this Contract the following words shall mean:-

"the Project"	accsc" "Certified Cyber Security Consultancy/'
"the Project Manager"	
"the Contractor's Project Manager"	"Commercially Sensitive Information"
	the project to be performed by the Contractor as described in Schedule One;
"the Act and the Regulations"	[redacted]Ground Floor, Sanctuary Buildings, 20 Great Smith Street, London SWIP 3BT [redacted]
"Affiliate"	[redacted]
"BPSS" "Baseline Personnel Security Standard"	means the Copyright Designs and Patents Act 1988 and the Copyright and Rights in Databases Regulations 1997;
	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;
"Common Criteria"	a level of security clearance described as pre-employment checks in the National Vetting Policy. Further Information can be found at: https://www.gov.uk/govemment/publications/governmentbaseline-personnel-security-standard;
"CCP" "Certified Professional"	the Common Criteria scheme provides assurance that a developer's claims about the security features of their product

are valid and have been independently tested against recognised criteria;	"Contracting Department"
is a NCSC scheme in consultation with government, industry and academia to address growing need for specialists in the cyber security profession and building a community of recognised professionals in both the UK public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certifiedprofessional:	"Contractor Personnel"
	"Contractor Software"
	"Control"
	"Controlled'
	"Copyright"
is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliersto deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy:	"Copyright Work"
	"CPA"
	"Commercial Product Assurance" [formerly called "CESG Product Assurance'l
	"Crown Body"
	"Cyber Essentials"
	"Cyber Essentials Plus"
information of a commercially sensitive nature relating to the Contractor, its IPR or its business or which the Contractor has indicated to the Department that, if disclosed by the Department, would cause the Contractor significant commercial disadvantage or material financial loss; "Confidential Information"	'Datal' means all information which has been designated as confidential by either party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including but not limited to information which relates to the business, affairs, properties, assets, trading practices, services, developments, trade secrets, Intellectual Property Rights, know-how, personnel, customers and suppliers of either party and commercially sensitive information which may be

regarded as the confidential information of the disclosing party;	
any contracting authority as defined in Regulation 5(2) of the Public Contracts (Works, Services and Supply) (Amendment) Regulations 2000 other than the Department;	
all employees, agents, consultants and contractors of the Contractor and/or of any Sub-contractor;	
software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services;	
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; take the meaning given in the GDPR;	
means any and all copyright, design right (as defined by the Act) and all other rights of a like nature which may, during the course of this Contract, come into existence in or in relation to any Work (or any part thereof);	
means any Work in which any Copyright subsists;	
	is an 'information assurance scheme' which evaluates commercial off the shelf (COTS) products and their developers against published security standards. These CPA certified products Can be used by government, the wider public sector and industry. See website: https://www.ncsc.gov.uk/scheme/commercial-productassurance-cpa:
	any department, office or agency of the Crown;
	Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme;
	There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers https://www.iasme.co.uk/apply-for-self-assessment/:
	means all data, information, text, drawings, diagrams, images or sound embodied in any electronic or tangible medium, and which are supplied or in respect of which access is granted to
	"Data Loss Event"
	"Data Protection Impact Assessment"
	"Data Protection Legislation"
	"Data Protection Officer' "Data Subject"
	"Data Subject Access Request"
	"Department Confidential Information"
	'Department's Data"
	"Department's Information"

	the Contractor by the Department pursuant to this Contract, or which the Contractor is required to generate under this Contract;
	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;
	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy; (iiii) all applicable Law about the processing of personal data and privacy; take the meaning given in the GDPR; take the meaning given in the GDPR;
	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;
	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;
	is any data or information owned or retained in order to meet departmental business objectives and tasks, including:
	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:
	(i) supplied to the Contractor by or on behalf of the Department; or
	(ii) which the Contractor is reqwred to generate, process, store or transmit pursuant to this Contract; or
	(b) any Personal Data for which the Department is the Controller;
"DfE"	means the Department for Education;
"Department"	
"Department Security Standards"	means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver
"Digital Marketplace/GCloud"	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT Health checks) are on the G-Cloud framework;
"DPA 2018"	Data Protection Act 2018;
"Effective Date"	the date on which this Contract is signed by both parties;
"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;

"FIPS 140-2"	this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled 'Security Requirements for Cryptographic Modules'. This document is the de facto security standard used for the accreditation of cryptographic modules;
'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 (EtJ) 2016/679);
"Good Industry Practice"	means the exercise of that degree of skill, care,
"Industry Good Practice"	prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;
"Good Industry Standard"	means the implementation of products and
"Industry Good Standard"	solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;
"GSC" "GSCP"	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/govemment/publications/governmentsecurity-classifications:
"HMG"	means Her Majesty's Government;
UICT'I	means Information and Communications Technology ('CT) 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;
"ICT Environment"	the Department's System and the Contractor System;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Intellectual Property Rights"	means patents, trade marks, service marks, design (rights whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or

"ISO/IEC 27001 " "ISO 27001 "

"ISO/IEC 27002" "ISO 27002"

"IT Security Health Check (ITSHC)"

"IT Health Check (ITHC)"

"Penetration Testing"

"LED"

"Malicious Software"

"Need-to-Know"

"NCSC'	information held on the IT system;
"OFFIcIAL"	Law Enforcement Directive (Directive (EU) 2016/680);
"OFFICIAL SENSITIVE"	any software program or code intended to destroy, interfere with, corrupts or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
	the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties;
	The National Cyber Security Centre (NCSC) formerly CESG Is the UK government's National Technical Authority for Information Assurance. The NCSC website is http://www.ncsc.gov.uk:
"Original Copyright Work"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services.
"Personal Data"	the 'OFFICIAL-SENSITIVE' caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy; means the first Copyright Work created in whatever form; take the meaning given in the GDPR; take the meaning given in the GDPR; take the meaning given in the GDPR;
"Personal Data Breach"	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;
"Processor"	"Regulatory Bodies"
"Protective Measures" business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom);	
is the International Standard describing the Code of Practice for Information Security Controls;	
is the International Standard describing the Code of Practice for Information Security Controls;	
means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of	"Request for Information"
	"Secure Sanitisation"

"Security and Information Risk Advisor' "CCP SIRA"	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations; Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation wilt allow you to re-use the media unuseabte. Secure sanitisation was previously covered by "Information Assurance Standard No.5 — Secure Sanitisation" ("IS") issued by the former CESG. Guidance can be found at: https://www.ncsc.gov.uk]quidance/secure-sanitisationstoraqe-media:
"SPF' "HMG Security Policy Framework"	The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction:
"Staff Vetting Procedures"	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-professionalscheme•
"Sub-Contractofl'	This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/qovemment/publications/security-policyframework
"Sub-processor' "Third Party Software"	the Department's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989; the third party with whom the Contractor enters into a Subcontract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents; any third Party appointed to process Personal Data on behalf of the Contractor related to this Contract; software which is proprietary to any third party [other than an Affiliate of the Contractor] which is or will be used by the Contractor for the purposes of providing the Services, and
'Work' 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;	means any and all works including but not limited to literary, dramatic, musical or artistic works, sound recordings, films, broadcasts or cable programmes, typographical arrangements and designs (as the same are defined in the Act) which are created from time to time during the course

	of this Contract by the Contractor or by or together with others at the Contractor's request or on its behalf and where such works directly relate to or are created in respect of the performance of this Contract or any part of it;
"Working Day"	any day other than a Saturday, Sunday or public holiday in England and Wales.

1 .2 References to "Contract" mean this contract (and include the Schedules). References to "Clauses" and "Schedules" mean clauses of and schedules to this Contract. The provisions of the Schedules shall be binding on the parties as if set out in full in this Contract.

1 .3 Reference to the singular include the plural and vice versa and references to any gender include both genders. References to a person include any individual, firm, unincorporated association or body corporate.

SCHEDULE ONE

1 BACKGROUND

The Government is interested in the potential that online learning, artificial intelligence and educational technology may have for upskilling and retraining large numbers of adults, particularly in intermediate skills.

This will be important as the labour market faces a number of challenges over the coming years, such as the growing automation of jobs, longer working lives and increasing the UK's productivity. This market study will explore the possible role of online learning and AIEd in helping to overcome these risks, and enabling people to re-skill and up-skill as the economy changes.

2 AIM

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

1. Describe the online learning and AIEd markets, and their economic structures.
2. Investigate whether the features of both respective markets are common to what we'd expect in one that is well-functioning.
3. Identify any barriers that prevent the markets from being well-functioning, and their causes.

3 OBJECTIVES

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

(b) Evaluate the current market for online intermediate skills courses for adults, which are accessible in England, including:

1. The market structure
2. The incentives that drive the behaviour of market participants
3. The volume of learners
4. The business models and cost structures
5. Pedagogical approaches
6. Whether there are market failures and their underlying causes

1. Evaluate the current and potential use of Artificial Intelligence in supporting online learning, including:

1.The ways in which it supports learners

2. The market structure
3. The business models and cost structures
4. Its effectiveness in upskiiling low-to-medium skilled adults
5. Past and future trends in development
6. Whether there are market failures and their underlying causes

4 TASKS

Task	Output	Date Re uired
Production of market assessment framework	ICF will conduct a rapid review of published market data and evidence, and produce a framework for assessing the market. This will be shared for DfE to comment rior to com letion	15th June
Production of research tools	ICF's project manager and director will design research toots to be used in later tasks. These tools will be: 1. A search strategy and extraction template for use in the mapping research; 2. Literature review protocols and extract templates for the literature review tasks; 3. A sampling strategy and DfE-headed letter for the recruitment of qualitative interviews; and 4. Topic guides for use in the conduct of the qualitative interviews This will be shared for DfE to comment prior to com letion	15th June
Mapping the online learning and AIEd markets	ICF will map existing online learning and AIEd provision to assess the size and characteristics of the markets, the actors within them, and the roducts the roduce	6th July
Interview recruitment	ICF will recruit 50 market actors for interview. This will include developers, providers and other market stakeholders, including independent expert academics. ICF will finalise the exact quotas with DfE before recruitin	20th July
Literature review	ICF will undertake a review of published literature relating to online learning and AIEd. The literature review will: 1. Provide further intelligence on the characteristics and functioning of the online learning and Al Ed markets 2. Assess the effectiveness of different forms of online learning and Al Ed	10th August
Conduct interviews	ICF will conduct face-to-face and telephone interviews with the market actors, using the topic uides a reed reviousl with DfE	10th August
Analysis	Analysis of the evidence collected through desk research and interviews will be collected in two waves. Firstly on week commencing 23rd July, to inform the interim report, and then week	W/C 23rd July and W/C 1 3th August

	commencing 13th August in order to inform the final re ort	
Interim report and presentation	ICF will produce a report of around 20 pages that will present the key findings from the mapping research, literature review and interview research that has been completed. Alongside the report, ICF will deliver a presentation of interim findings for w/c 6th Au ust	10th August
Skeleton report	ICF will submit a skeleton report to DfE, which will include detailed section and subsection fans, which	24th August
	describe the intended content and length of each. ICF will allow at least a week for DfE to review	
Initial draft report	ICF will produce a 30-40 page report that presents the synthesised findings from all the completed research and analysis. It will include detailed sections on: 1. The characteristics, size and structure of the markets 2. The conduct of the markets 3. Behaviour of market actors and factors influencing this 4. Wider funding and technology drivers affecting the markets now and in future 5. Performance of the markets 6. Assessment of the functioning of the markets 7. Conclusions and recommendations on the possible role Government can play	7th September
Final report	Following comments from the DfE steering group on the draft report, ICF will schedule a call with the DfE project manager to review and agree revisions to the report, before submitting a final report produced in the DfE tem late	28th September

5 STAFFING

ICF staff

Ali Zaidi will be the PM for this project, and the day-to-day contact for DfE. He will manage the team's inputs, undertake research tasks, produce the research tools and will be the lead author for all reporting outputs.

Shane Beadle be' the Project Director. He will and be able to respond to the client in the event of any serious technical, management or contractual issue.

To mitigate the risk of the Project Manager or Project Director needing to be replaced, Colin Howat will be the deputy project director and Tim Knight will be the deputy project manager.

DfE staff

Jaimin Tailor witl be the Project manager for this project and the day-to-day contact for ICF. He will provide support throughout the project and will chair and facilitate the steering committee which will provide comments on behalf of the Department's interested policy and analytical teams.

6 STEERING COMMITTEE

The Project Manager shall set up a Steering Committee for the Project, consisting of representatives from the Department, the Contractor, and any other key organisations whom the project will impact on, to be agreed between the parties. The function of the Steering Committee shall be to review the scope and direction of the Project against its aims and objectives, monitor progress and efficiency, and assess, manage and review expected impact and use of the findings from the Project against an agreed Project Communication Plan, through the standard Department Communication Plan Template. The Committee shall meet at times and dates agreed by the parties, or in the absence of agreement, specified by the Department. The Contractor's representatives on the Steering Committee shall report their views on the progress of the Project to the Steering Committee in writing if requested by the Department. The Contractor's representatives on the Steering Committee shall attend all meetings of the Steering Committee unless otherwise agreed by the Department.

7 RISK MANAGEMENT

Risk	Likelihood / Impact	Mitigating Actions
Research tasks are not completed within the planned timescales leading to a failure to deliver reporting outputs by required deadlines.	Med / High	1. The project team has been selected to enable research tasks to be completed in parallel. 2. Team members' have the capacity to carry out the tasks in this proposal; time will be ring-fenced for the Completion of all tasks on commissioning. 3. The Project Manager will monitor progress and completion of tasks on a weekly basis and allocate additional staff resource if a task starts to fall behind schedule. ICF have other team members who could be drawn in.
Data on developer / provider websites is presented in differing formats compromising our ability to complete the mapping exercise in planned timescales.	Med / Low	4. Data recording templates for use in the mapping exercise will be designed to accommodate some variation in the data available. 5. Templates will also initially be piloted and adjusted if necessary to ensure a balance between the comprehensiveness of the data being recorded and the efficiency of the recording process.

The literature review finds a shortage of robust empirical evidence, making it difficult to draw any firm conclusions about the effectiveness of online learning and AIEd.	Med / Med	6. Potential literature review sources concerning effectiveness will be assessed on the Maryland scale but ICF do not propose to automatically exclude sources scoring below 4 or 5. 7. ICF will share their initial assessment of the robustness of potential sources with DfE and, if a shortfall is identified, ICF WOUEd recommend the inclusion of lower scoring sources (e.g. qualitative studies) if these can usefully provide additional narrative and indicative evidence to complement more robust sources.
The research does not account for the diversity in the market, meaning findings are not representative.	Low / Med	8. The sampling strategies for the qualitative fieldwork will be designed to ensure different types and subgroups are represented. 9. Recruitment quotas will be set for developers of different forms of online learning and providers offering different levels and models of provision.
Developers and/or providers are reluctant to disclose financial information, resultin in a lack of	Low / Med	10. As ICF have successfully done on other occasions, potential participants in the research will be given clear reassurances when they are first contacted about the confidentiality anonymity of the research.
insight into how the market functions.		11. These reassurances will also be reiterated at the start of each interview.
Reporting outputs do not accurately convey findings, undermining the ability of the research to inform future policy.	Low / Med	• All outputs will be drafted by the Project Manager and quality assured by the Project Director. • Detailed report plans will also be prepared in advance and shared with DfE for comment/discussion.
fLR data takes longer than anticipated to be delivered to ICF	Med / Low	12. The project has been structured such that II-R data is not most needed until the analysis phase in July and August — and ICF have previous experience of successful II-R requests in short timeframes.

8 DATA COLLECTION

The Department seeks to minimise the burdens on Schools, Children's Services and Local Authorities (LAS) taking part in surveys.

When assessing the relative merits of data collection methods the following issues should be considered;

1. only data essential to the project shall be collected;
2. data should be collected electronically where appropriate/preferred;

3. questionnaires should be pre-populated wherever possible and appropriate;
4. schools must be given at least four working weeks to respond to the exercise from the date they receive the request; and
5. LAS should receive at least two weeks, unless they need to approach schools in which case they too should receive 4 weeks to respond;

The Contractor shall clear any data collection tools with the Department before engaging in field work.

The Contractor shall check with the Department whether any of the information that they are requesting can be provided centrally from information already held.

9 CONSENT ARRANGEMENTS

The Department and the contractor shall agree in advance of any survey activity taking place the consent arrangements that shall apply for each of the participant groups. All participants should be informed of the purpose of the research, that the Contractor is acting on behalf of the Department and that they have the option to refuse to participate (opt out). Contact details should be provided including a contact person at the Department. Children who are 16 or over will usually be able to give their own consent but even where this is so, the Contractor, in consultation with the Department, should consider whether it is also appropriate for parents, guardians or other appropriate gatekeepers (e.g. schools, Local Authorities) to be informed when a child has been invited to participate in research.

10 PROJECT COMMUNICATION PLAN

The Contractor shall work with the Project Manager and Steering Group to agree the content of the Project Communication Plan on the standard Department Communication Plan Template at the start of the Project, and to review and update at agreed key points in the Project and at the close of the Project. The Communication Plan shall set out the key audiences for the Project, all outputs intended for publication from the Project, the likely impact of each output, and dissemination plans to facilitate effective use by the key audiences.

End of Schedule One

SCHEDULE MO

1 Eligible expenditure

1.1 The Department shall reimburse the Contractor for expenditure incurred for the purpose of the Project, provided that:-

(a) the expenditure falls within the heading and limits in the Table below; and

1. the expenditure is incurred, and claims are made, in accordance with this Contract.

Table

Pro•ect Milestone	Pa ment Amount	Pa ment Date
Production of market assessment framework	[redacted](excluding VAT)	W/C 18th June
Interim Re ort	[redacted]excludin VAT	w/c 13th Au ust
Final Re ort	[redacted]excludin VAT	w/c 24th Se tember

Total Project expenditure shall not exceed £49,550 exclusive of VAT.

2 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 Project 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 accounts 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.

10. Invoices shall be submitted on the invoice dates specified in the Table, be detailed against the task headings set out in the Table and must quote the Department's Order Number. The Purchase order reference number shall be provided by the department when both parties have signed the paperwork. The Contractor or his or her nominated representative or accountant shall certify on the invoice that the amounts claimed were expended wholly and necessarily by the Contractor on the Projects 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.

11. Invoices shall be sent to the Department for Education, PO Box 407, SSCL, Phoenix House, Celtic Springs Business Park, Newport, NPIO 8FZ and/or by email to APinvoices-DFE-U@sscl.gse.gov.uk. Invoices submitted by email must be in PDF format, with one PDF file per invoice including any supporting documentation in the same file. Multiple invoices may be submitted in a single email but each invoice must be in a separate PDF file. The Department undertakes to pay correctly submitted invoices within 10 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 may 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 Project Manager. The Department aims to reply to complaints within 10 working days. The Department shall not be responsible for any delay in payment caused by incomplete or illegible invoices.

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

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

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

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

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

End of Schedule Two

SCHEDULE THREE

1. Contractor's Obligations

1.1. The Contractor shall promptly and efficiently complete the Project in accordance with the provisions set out in Schedule One.

1.4The Contractor shall comply with the accounting and information provisions of Schedule Two.

1.5The 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.

1.6The Contractor shall inform the Department immediately if it is experiencing any difficulties in meeting its contractual obligations.

2 Department's Obligations

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

3 Changes to the Department's Requirements

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

3.4 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.

4 Management

4.3 The Contractor shall promptly comply with ail reasonable requests or directions of the Project Manager in respect of the Services.

4.4The Contractor shall address any enquiries about procedural or contractual matters in writing to the Project Manager. Any correspondence relating to this Contract shall quote the reference number set out in the Recitals to this Contract.

5 Contractor's Employees and Sub-Contractors

5.1 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 5.1. Unless otherwise agreed by the Department in writing, the Contractor shall ensure that any contract requiring payment to a Subcontractor 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:

5.1.1 10 days, where the Sub-contractor is an SME; or

5.1.2 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.

5.2 The Department shall be entitled to withhold payment due under clause 5.1 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 5.1. For the avoidance of doubt the Department shall not be liable to pay any interest or penalty in withholding such payment.

1. 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.

2. 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.

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

4. If the Department notifies the Contractor that it considers that an employee or sub-contractor is not appropriately qualified or trained to perform the Project or otherwise is not performing the Project 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 performing the Project and shall provide a suitable replacement (at no cost to the Department).

5. The Contractor shall take all reasonable steps to avoid changes of employees or sub-contractors assigned to and accepted to perform the Project under the Contract except whenever changes are unavoidable or of

a temporary nature. The Contractor shall give at least four week's written notice to the Project Manager of proposals to change key employees or subcontractors

13.Ownership of Intellectual Property Rights, Copyright & Licence to the Department

1. Ownership of Intellectual Property Rights including Copyright, in any guidance, specifications, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models ,designs or other materials prepared by or for the Contractor on behalf of the Department for use, or intended use, in relation to the performance by the Contractor of its obligations under the Contract shall belong to the Contractor
2. The Contractor hereby grants to the Department a non-exclusive license without payment of royalty or other sum by the Department in the Copyright to:
   - 6.2.1 to do and authorise others to do any and all acts restricted by the Act as amended from time to time or replaced in whole or part by any statute or other legal means in respect of any Copyright Work in the United Kingdom and in all other territories in the world for the full period of time during which the Copyright subsists; and

6.22 to exercise all rights of a similar nature as those described in Clause 6.2.1 above which may be conferred in respect of any Copyright Work by the laws from time to time in all other parts of the world

6.3 The Contractor now undertakes to the Department as follows:

6.3.1 not to assign in whole or in part the legat or beneficial title in any Copyright to any person, firm or company without the prior written consent of the Department the granting of which consent shall be at its absolute discretion.

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

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

6.3.4 in respect of the Original Copyright Works to:

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

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

6.37 to take all necessary steps and use its best endeavours to prevent the infringement of the Copyright by any person, firm or company which shall include an obligation on the part of the Contractor to commence and prosecute legal proceedings for any threatened or actual infringement where there is a reasonable chance of success and account to the Department after

the deduction of all legal expenses incurred in any such proceedings for one half of all damages paid whether by order, settlement or otherwise.

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

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

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

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

6.5 The warranty and indemnity contained in Clause 6.4.1 above shall survive the termination of this Contract and shall exist for the life of the Copyright.

7.Data Protection Act

7.1 . The Parties acknowledge that for the purposes of the Data Protection Legislation, the Department is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is listed in Schedule 4 by the Department and may not be determined by the Contractor.

7.2. The Contractor shall notify the Department immediately if it considers that any of the Department's instructions infringe the Data Protection Legislation.

7.3. The Contractor shall provide all reasonable assistance to the Department in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Department, 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.

7.4. The Contractor 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 4, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Department before processing the Personal Data unless prohibited by Lavv
- (b) ensure that it has in place Protective Measures in accordance with Schedule 5, which have been reviewed and approved by the Department as appropriate to protect against a Data Loss Event 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 Contractor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule

  (ii)it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:
- (A) are aware of and comply with the Contractor's duties under this clause;
- (B) are subject to appropriate confidentiality undertakings with the
  Contractor 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 Department 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 Department has been obtained and the following conditions are fulfilled:
  (i)the Department or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Department;
- (ii) the Data Subject has enforceable rights and effective legal remedies;
- (iii) the Contractor 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 Department in meeting its obligations)' and

- (iv) the Contractor complies with any reasonable instructions notified to it in advance by the Department with respect to the processing of the Personal Data; (e)at the written direction of the Department, delete or return Personal Data (and any copies of it) to the Department on termination of the Contract unless the Contractor is required by Law to retain the Personal Data.

7.5. Subject to clause 7.6, the Contractor shall notify the Department immediately if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access 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.

7.6. The Contractor's obligation to notify under clause 7.5 shall include the provision of further information to the Department in phases, as details become available.

7.7. Taking into account the nature of the processing, the Contractor shall provide the Department with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 7.5 (and insofar as possible within the timescales reasonably required by the Department) including by promptly providing:

- (a) the Department with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Department to enable the Department to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation; • (c) the Department, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Department following any Data Loss Event; (e)assistance as requested by the Department with respect to any request from the Information Commissioner's Office, or any consultation by the Department with the Information Commissioners Office.

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

- (a) the Department determines that the processing is not occasional; • (b) the Department 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 Department determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

7.9. The Contractor shall allow for audits of its Data Processing activity by the Department or the Department's designated auditor. , which is not a competitor of Contractor.

7.10. The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

7.1 1. Before allowing any Sub-processor to process any Personal Data related to this Contract, the Contractor must:

(a) notify the Department in writing of the intended Sub-processor and processing;

- (b) obtain the written consent of the Department;
- (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause such that they apply to the Subprocessor; and
- (d) provide the Department with such information regarding the Subprocessor as the Department may reasonably require.

7.12. The Contractor shall remain fully liable for all acts or omissions of any Subprocessor.

7.13. The Contractor may, at any time on not less than 30 Working Days' notice, revise this clause by replacing itwith 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).

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

14.Departmental Security Standards

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

8.2. Where the Contractor will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Department, the requirements under Cabinet Office Procurement Policy Note — Use of Cyber Essentials Scheme certification - Action Note 09/14 25 May 2016, or any subsequent updated document, are mandated; that "contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme". The certification scope must be relevant to the services supplied to, or on behalf of, the Department.

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

8.4 The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).

8.5 Departmental Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Contractor's or subcontractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Departmental Data then the Contractor and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.

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

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

8.8 The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.

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

8.10 Storage of Departmental Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.1 1 and 1.12 below.

8.1 1 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or (sub„)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPSI 40-2 standard or another encryption standard that is acceptable to the Department.

8.12 All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Departmental Data to deliver and support the service, shall be under the control and configuration management of the contractor or subcontractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPSI 40-2 standard or another encryption standard that is acceptable to the Department.

8.13 Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

8.14 When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

8.15 At the end of the contract or in the event of equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Contractor's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Contractor or subcontractor shall protect the Department's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

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

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

8.18 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.

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

8.20 The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.

8.21 The Contractor or sub-contractors providing the service will provide the Department with full details of any storage of Departmental Data outside of the UK or any future intention to host Departmental Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Contractor or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Department.

8.22 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.

8.23 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.

8.24. The Contractor and sub-contractors shall undergo appropriate security assurance activities as determined by the Department. Contractor and subcontractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractors security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA).

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 Project 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 Project 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 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 Project is not performed in accordance with this Contract then the Department shall be entitled, where appropriate to:

9.21. require the Contractor promptly to re-perform or replace the relevant part of the Project without additional charge to the Department; or

9.22. 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 performance of the Project.

9.4 Without prejudice to any other exclusion or limitation of liability in this Contract, the liability of the Contractor for any claim or claims under this Contract shall be limited to such sums as it would be just and equitable for the Contractor to pay having regard to the extent of his responsibility for the loss or damage giving rise to such claim or claims etc.

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, it's 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.

12. Termination

12.1. This Contract may be terminated by either party giving to the other party at least 30 days notice in writing.

12.2. 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.

12.3. 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.

12.4. 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;

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

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

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

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

13. 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. Freedom of information

12.1 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.

12.2 The Contractor shall and shall procure that its Sub-contractors shall:

122.1 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;

12.22 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

12.2.3 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.

12.3 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.

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

12.5 The Contractor acknowledges that (notwithstanding the provisions of Clause 1 3) 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:

12.5.1 in certain circumstances without consulting the Contractor; or

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

125.3 provided always that where 125.1 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.

12.6 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.

13. CONFIDENTIALITY

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

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

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

13.2 Clause 13 shall not apply to the extent that:

13.2.1 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 12 (Freedom of Information);

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

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

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

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

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

13.4 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.

13.5 At the written request of the Department, the Contractor shall procure that those members of the Contractor Personnel identified in the Department's notice signs a confidentiality undertaking prior to commencing any work in accordance with this Contract.

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

13.6.1 to any Crown Body or any other Contracting Department. All Crown Bodies or Contracting Authorities receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other Crown Bodies or other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Department;

13.6.2 to any consultant, contractor or other person engaged by the Department or any person conducting an Office of Government Commerce gateway review;

13.6.3 for the purpose of the examination and certification of the Department's accounts; or

13.6.4 for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Department has used its resources.

13.7 The Department shall use all reasonable endeavours to ensure that any government department, ContraCting Department, employee, third party or Sub-contractor to whom the Contractors Confidential Information is disclosed pursuant to clause 13 is made aware of the Department's obligations of confidentiality.

13.8 Nothing in this clause 13 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 IPR.

13.9 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.

13.10 Subject to Clause 13.9, the Contractor hereby gives his 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.

13.11 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.

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

14. Access and Information

14.1 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 that may adversely affect the ability of the Department to ensure an orderly transfer of responsibility.

16. Tax indemnity

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

16.2 Where the Contractor is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall

at all times comply with the Social Security Contributions and Benefits Act 1992
(SSCBA) and atl other statutes and regulations relating to NICs in respect of that consideration.

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

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

16.5 The Department may terminate this contract if-

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

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

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

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

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

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

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

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

Contractor to its officers or employees in connection with this Contract.

16.9 The Contractor shall indemnify Department against any liability, assessment or claim made by the HM Revenue and Customs or any other relevant authority arising out of the perfomance 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. Amendment and variation

17.1 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 that the Department may have in place from time to time.

18. Assignment and Sub-contracting

18.1 The benefit and burden of this Contract may not be assigned or subcontracted 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.

19. The Contract (Rights of Third Parties) Act 1999

19.1 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.

20. Waiver

20.1 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.

21. Notices

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

22. Dispute resolution

22.1 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.

22.2 Any dispute not capable of resolution by the parties in accordance with the terms of Clause 21 shall be settled as far as possible by mediation in accordance with the Centre for Dispute Resolution (CEDR) Model Mediation Procedure.

22.3 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.

23. Law and Jurisdiction

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

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, Safeguarding children who participate in research

25.1 The Contractor will put in place safeguards to protect children from a risk of significant harm which could arise from them taking part in the Project. The Contractor will agree these safeguards with the Department before commencing work on the Project.

25.2 In addition, the Contractor will carry out checks with the Disclosure and Barring Service (DBS checks) on all staff employed on the Project in a Regulated Activity. Contractors must have a DBS check done every three years for each relevant member of staff for as long as this contract applies. The DBS check must be completed before any of the Contractor's employees work with children in Regulated Activity. Please see https://www.gov.uk/crb-criminal-records-bureau-check for further guidance.

26. Project outputs

26.1 Unless otherwise agreed between the Contractor and the Project Manager, all outputs from the Project shall be published by the Department on the Department's research website.

26.2 The Contractor shall ensure that all outputs for publication by the Department adhere to the Department's Style Guide and MS Word Template, available to download from: https://www.gov.uk/government/publications/eoi-guide

26.3 Unless otherwise agreed between the Contractor and Project Manager, the Contractor shall supply the Project Manager with a draft for comment at least eight weeks before the intended publication date, for interim reports, and eight weeks before the contracted end date, for final reports.

26.4 The Contractor shall consider revisions to the drafts with the Project Manager in the light of the Department's comments. The Contractor shall provide final, signed off interim reports and other outputs planned within the lifetime of the Project to the Department by no later than four weeks before the intended publication date, and final, signed off reports and other outputs at the end of the Project to the Department by no later than the contracted end date for the Project.

26.5 Until the date of publication, findings from all Project outputs shall be treated as confidential, as set out in the Clause 13 above. The Contractor shall not release findings to the press or disseminate them in any way or at any time prior to publication without approval of the Department.

26.6 Where the Contractor wishes to issue a Press Notice or other publicity material containing findings from the Project, notification of plans, including timing and drafts of planned releases shall be submitted by the Contractor to the Project Manager at least three weeks before the intended date of release and before any agreement is made with press or other external audiences, to allow the Department time to comment. All Press Notices released by the Department or the Contractor shall state the full title of the research report, and include a hyperlink to the Department's research web pages, and any other web pages as relevant, to access the publication/s. This clause applies at all times prior to publication of the final report,

26.7 Where the Contractor wishes to present findings from the Project in the public domain, for example at conferences, seminars, or in journal articles, the Contractor shall notify the Project Manager before any agreement is made with external audiences, to allow the Department time to consider the request. The Contractor shall only present findings that will already be in the public domain at the time of presentation, unless otherwise agreed with the Department. This clause applies at all times prior to publication of the final report.

End of Schedule Three

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

Signature

Name in CAPITALS

[redacted]

Position and Address

Deputy Director,
Skills Policy Analysis,
Department for Education,
20 Great Smith Street, London,
SW1P 3BT

Date 02/08/18

Authorised to sign for and on behalf of the Contractor

Signature

Name in CAPITALS

Position and Address

Senior Commercial Manager, ICF

Date 30/07/18

Schedule 5 Contractor Technical and Operational Measures

Roles of the Parties.

1. During the Term of this Agreement, the Parties agree to comply with Data Protection Legislation directly applicable to their respective businesses.
2. As between the Parties for the Processing of Authority Personal Data, the Parties will be joint Data Controller and the Contractor shall be the Data Processor. The Parties will be responsible for determining their respective compliance with Data Protection Legislation as the Data Controller. The Contractor shall be responsible for determining compliance with Data Protection Legislation as the Data Processor.
3. In no event will either Party be required to monitor or advise the other regarding the Data Protection Legislation applicable to other Party with respect to Authority Personal Data.
4. The Contractor will provide verifiable notice to the Authority's, employees, or other applicable Data Subjects through the Contractor's applicable local country privacy statement. Such privacy statement must comply with applicable Data Protection Legislation. In the event of a conflict between the Contractor's local country privacy statement and the terms of any agreement(s) between the Parties for Services, the terms of this Agreement will control.
5. The Contractor will obtain Data Subject verifiable, freely given, specific and unambiguous consent to process Authority Personal Data in the Services.

15. Security Controls and Safeguards

1. The Contractor maintains commercially unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Authority Personal Data), confidentiality and integrity of Authority Personal Data during the Term and as long as Authority Personal Data is in the Contractor's possession or under the Contractor's control. The Contractor regularly monitors network and production systems and implements and maintains security controls and procedures designed to prevent, detect and respond to identified threats and risks in order to reasonably assess and prevent unauthorized access to or unauthorized use of Authority Personal Data, and upgrade information safeguards as necessary to limit risks. Such controls include, but are not limited to:
   1. Security Data Protection Awareness and Training. The Contractor requires and will continue to require annual securtty and privacy training for all personnel with access to Authority Personal Data.
   2. Background Checks. The Contractor shall perform a criminal background check on any employee performing Contractor Services under the Agreement.
   3. Access Limitations. The Contractor i) limits access to its information systems and the facilities in which they are housed to authorized persons under the Agreement and to those persons who are reasonably required to know such information to perform the Services and ii) subjects such authorized persons to user authentication and log on processes when they need access to Authority Personal Data. Such access shall be accompanied by, at a minimum, a written procedure that sets forth the manner in which access to

reasonable and appropriate administrative, organizational technical and security measures designed to protect the security (including protection against unauthorized or unlawful Processing and against accidental or Personal Data upon employment termination or a change in job status that results in the personnel no longer requiring access to Authority Personal Data.

4. Passwords and Encryption. The Contractor i) requires strong password standards (8 characters minimum), which include length, complexity and expiration; ii) blocks access after attempt threshold is met; and ii) encrypts access to Authority Personal Data during transmission over the Internet.
5. Monitoring, Testing and Detection. The Contractor: i) employs an industry standard network intrusion detection system and firewalls to monitor and block suspicious network traffic; ii) reviews access logs on servers and security events and retaining network security logs for 180 days; iii) reviews privileged access to production systems; iv) performs network vulnerability assessments on a regular basis. Scans will be performed using commercially available scanning tools that identify application and operating system vulnerabilities; v) maintains a vulnerability remediation program; v) makes sure all endpoints run an anti-virus solution and applies timely signature updates; vi) patches all critical, exploitable vulnerabilities in a commercially reasonable manner; and vi) engages, upon the Authority's prior written instruction, third parties to perform network penetration testing on at least an annual basis.
6. Remediation and Response. The Contractor: i) documents responsive actions taken regarding any data protection incident and implements mandatory post-incident review of events and actions taken, if any, to change business practices relating to protection of Authority Personal Data.

Authority Personal Data is restricted, and storage of the Authority Personal Data in locked facilities, storage areas or containers; and ii) removes the Contractor personnel access to Authority

16. Business Continuity and Disaster Recovery

1. Emergency Policies and Procedures. The Contractor has policies and procedures in place for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic, and natural disaster) that could damage Authority Personal Data or production systems that contain Authority Personal Data.
2. Network and Storage Redundancy. The Contractor commissions the design and build of network and storage components for high availability, including, but not limited to all network devices (firewalls, load balancers, switches, and Internet connectivity, through multiple connections to ensure application availability and protect information from accidental loss or destruction.
3. Disaster Recovery Plan. The Contractor's Disaster Recovery plan incorporates failover between its EEA and UK data centres. Service restoration is within commercially reasonable efforts and is performed in conjunction with a data centre provider's ability to provide adequate infrastructure at the prevailing failover location.
4. Data Centres and Processes. The Contractor relies on reputable data centre providers' multiple levels of power redundancy,

uninterrupted power supply (UPS) and backup power for the Contractor's system containing Authority Personal Data. The UPS power subsystem is redundant, with instantaneous failover if the primary UPS fails. Data centre facilities containing Authority Personal Data are environmentally controlled to ensure airflow, temperature and humidity levels.

17. Backup and Recovery.

5.1 The Contractor, upon the Authority's prior written instruction, will make sure that: i) data centre facilities utilise snapshot and data mirroring capabilities; ii) backup data is not transferred cross border; iii) the integrity of local backups is tested monthly by restoring a complete database from a selected snapshot copy to test systems and validate the data integrity; and iv) this process is undertaken for offsite backups on a quarterly basis.

Data Breach to the extent the remediation

18. Authority Personal Data Incident is within the Contractor's reasonable Management, Notification and Related control.

Process. 4. In the event of a Personal Data Breach, the 1 . Notification and Updates. The Contractor Contractor shall not inform any third party shall notify the Authority without undue without first obtaining the Authority's prior delay after becoming aware of the written consent, unless notification is suspected or actual accidental or required by Data Protection Legislation or unlawful destruction, loss, alteration, any other law to which the Contractor is unauthorized disclosure of, or access to subject, in which case the Contractor Authority Personal Data by the shall to the extent permitted by such law Contractor, the Contractor Affiliates or inform the Authority of that legal Contractor Sub-processors ("Authority requirement, provide a copy of the Personal Data Breach") of which the proposed notification and consider any

Contractor becomes aware ("Authority comments made by that Authority before Personal Data Breach Notice"). The notifying any third party of the Personal obligations within this Section shall not Data Breach. apply to incidents that are caused by the Authority.

2. Authority Personal Data Breach Notice. Such notification, will, at minimum,: (i) describe the nature of the Authority Personal Data Breach, including the date of the Authority Personal Data Breach and the date of the discovery; (ii) describe the types of Authority Personal Data involved, including the number and categories or identities of Data Subjects involved; (iii) communicate the name and contact details of the Contractor's data protection officer, chief information security officer or other relevant contact from whom more information may be obtained; (iv) describe the measures the Contractor has taken, is taking, and intends to take to mitigate harm or remediate the Authority Personal Data Breach; and (v) recommend steps that the Authority should take to protect any affected individuals from harm. The Contractor will promptly update

information provided in the Authority Personal Data Breach Notice to the Authority.

3. Investigation and Cooperation. The Contractor shall make reasonable efforts to cooperate with the Authority to identify the cause of such Authority Personal Data Breach and take those steps as the Contractor deems necessary and reasonable to investigate and remediate the cause of such an Authority Personal