www.cqc.org.uk

Contract

Contract for the provision of Literature Review: Public Engagement

Contract Reference CQC AM 157

September 2018

Contents

THIS CONTRACT is dated 19 September 2018

PARTIES

(1) **CARE QUALITY COMMISSION** of 151 Buckingham Palace Road, London, SW1W 9SZ (**"Authority"**)

and

(2) **UNIVERSITY OF PLYMOUTH ENTERPRISE LIMITED** a wholly owned subsidiary of University of Plymouth a private company limited by shares with company number 03707827 of New Cooperage Building, Royal William Yard, Plymouth, PL4 8AA (**"Contractor"**)

(Together the **"Parties"**)

Background

1. The Authority is the independent health and social care regulator in England that monitors, inspects and regulates health and social care services to ensure they meet fundamental standards of quality and safety. It ensures health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve.

2. The Contractor has been appointed by the Authority to provide the Services (as defined below).

3. Therefore the Parties have agreed to enter into this Contract for the provision of the services defined in the Specifications.

1 Interpretation

1.1 In these terms and conditions:

"Agreement"	means the contract consisting of these terms and conditions, any attached Schedules, the invitation to tender including Specification, the Tender Response and Award Letter between (i) the Care Quality Commission ("Authority") and (ii) University of Plymouth Enterprise Limited ("Contractor");
"Approval"	means the written consent of the Authority;
"Authority"	means the Care Quality Commission;
"Authority Data"	means: (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 Authority; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to the Contract; or (b) any Personal Data for which the Authority is the Data Controller;
"Breach of Security"	means the occurrence of unauthorised access to or use of the Premises, the Services, the Contractor system, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.
"Central Government Body"	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:

	(a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;
"Charges"	means the charges for the Services as specified in the Schedule 2;
Change Control Notice ("CCN")	means a change control notice in the form set out in Schedule 6;
"Confidential Information"	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
"Contract"	means this Agreement;
"Contractor"	means the person named as Contractor who was awarded this Contract;
"Contract Period"	means the Term of this Contract including any period of extension;
"Contractor Personnel/Staff"	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement;
"Data Controller, Data Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer"	shall each have the same meaning given in the GDPR;

"Data Protection Legislation	means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii) the DPA 2018 to the extent that it relates to the processing of Personal Data and privacy; (iii) all applicable Law about the processing of Personal Data and privacy;
"Data Loss Event"	means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;
"Data Protection Impact Assessment"	means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Default"	means any breach of the obligations of the relevant Party (including abandonment of the Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of the Contract and in respect of which such Party is liable to the other;
"DPA"	means the Data Protection Act 2018 and any subordinate legislation made under that 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;
"Expiry Date"	means the date for expiry of the Agreement as set out in clause 4.1;
"FOIA"	means the Freedom of Information Act 2000;
"GDPR"	means the General Data Protection Regulation (*Regulation (EU) 2016/679*;

"Information"	has the meaning given under section 84 of the FOIA;
"Key Personnel"	means any persons specified as such in the Specification or Agreement otherwise notified as such by the Authority to the Contractor in writing;
"Law"	means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply;
"LED"	means Law Enforcement Directive (*Directive (EU) 2016/680*)
"Loss"	means any losses, costs, charges, expenses, interest, fees (including legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, charges, fines, damages, destruction, adverse judgments, orders or other sanctions and the term "**Losses**" shall be construed accordingly;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, 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;
"Party"	means the Contractor or the Authority (as appropriate) and "Parties" shall mean both of them;
"Premises"	means the location where the Services are to be supplied, as set out in the Specification;
"Prohibited Act"	the following constitute Prohibited Acts: • to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: (i) induce the person to perform improperly a relevant function or activity; or (ii) reward that person for improper performance of a relevant function or activity;

- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this agreement;
- committing any offence: (i) under the Bribery Act; (ii) under legislation or common law concerning fraudulent acts; or (iii) defrauding, attempting to defraud or conspiring to defraud the Authority;
- any activity, practice or conduct which would constitute one of the offences listed under (a) to (c), if such activity, practice or conduct had been carried out in the UK.

"Protective Measures"	means appropriate technical and organisational measures which 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;
"Purchase Order Number"	means the Authority's unique number relating to the supply of the Services by the Contractor to the Authority in accordance with the terms of the Agreement;
"Relevant Requirements"	means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"Request for Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "request" shall apply);
"Schedule"	means a schedule attached to, and forming part of, the Agreement;
"Security Policy"	means the Authority's Information Security and Governance Policy appended to Schedule 5 instead of 'ISO/IEC 27001';

"Security Plan"	means the Contractor's security plan prepared pursuant to paragraph 3 of Schedule 5, an outline of which is set out in an Appendix to Schedule 5
"Security Policy Framework"	means the HMG Security Policy Framework (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf)
"Services"	means the services to be supplied by the Contractor to the Authority under the Agreement;
"Specification"	means the specification for the Services (including as to quantity, description and quality) as specified in the Award Letter and appended hereto in Schedule 1;
"Staff"	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor engaged in the performance of the Contractor's obligations under the Agreement;
"Staff Vetting Procedures"	means vetting procedures that accord with good industry practice or, where requested by the Authority, the Authority's procedures for the vetting of personnel as provided to the Contractor from time to time;
"Sub-processor"	means any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement;
"Supplier Code of Conduct"	means HM Government Supplier Code of Conduct dated September 2017
"Term"	means the period from the start date of the detailed in clause 4.1 to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement;
"Third Party Software"	means software which is proprietary to any third party which is or will be used by the Contractor to provide the Services including the software and which is specified as such in Schedule 7;

"VAT"	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
"Variation"	means a variation to the Specification, the Price or any of the terms and conditions of the Contract;
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

1.2 In these terms and conditions, unless the context otherwise requires:

1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;

1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;

1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and

1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Priority of documents

2.1 In the event of, and only to the extent of, any conflict between the clauses of the Agreement, any document referred to in those clauses and the Schedules, the conflict shall be resolved in accordance with the following order of precedence:

a) these terms and conditions

b) the Schedules

c) any other document referred to in these terms and conditions

3 Supply of Services

3.1 In consideration of the Authority's agreement to pay the Charges, the Contractor shall supply the Services to the Authority for the Term subject to and in accordance with the terms and conditions of the Agreement.

3.2 In supplying the Services, the Contractor shall:

3.2.1 co-operate with the Authority in all matters relating to the Services and comply with all the Authority's reasonable instructions;

3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Contractor's industry, profession or trade;

3.2.3 use Staff who are suitably skilled, experienced and possess the required qualifications to perform tasks assigned to them, and in sufficient number to ensure that the Contractor's obligations are fulfilled in accordance with the Agreement;

3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;

3.2.5 comply with all applicable laws; and

3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.

3.3 The Authority may by written notice to the Contractor at any time request a Variation to the scope of the Services. If the Contractor agrees to any Variation to the scope of the Services, the Charges shall be subject to fair and reasonable adjustment to be agreed in writing between the Authority and the Contractor prior to the commencement of such Variation.

3.4 Any Variation will not take effect unless recorded in a Change of Control Notice as attached hereto in Schedule 6 and approved in writing by the Authority.

4 Term

4.1 The Agreement shall take effect on the date 19 September 2018 and shall expire on the Expiry Date of 30 November 2018, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.

4.2 Subject to clauses 3.3, 3.4 and 20.3, the Authority may request an extension to the Agreement for a period of up to 6 months by giving not less than 30 Working Days' notice in writing to the Contractor prior to the Expiry Date. The terms and conditions of the Agreement shall apply throughout any such extended period.

5 Charges, Payment and Recovery of Sums Due

5.1 The Charges for the Services shall be as set out in Schedule 2 and shall be the full and exclusive remuneration of the Contractor in respect of the supply of the Services. Unless otherwise agreed in writing by the Authority, the Charges shall include every cost and expense of the Contractor directly or indirectly incurred in connection with the performance of the Services.

5.2 The Contractor shall invoice the Authority as specified in the Agreement. Each invoice shall include such supporting information required by the Authority to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.

5.3 In consideration of the supply of the Services by the Contractor, the Authority shall pay the Contractor the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number. The Authority may, without prejudice to any other rights and remedies under the Agreement, withhold or reduce payments in the event of unsatisfactory performance.

5.4 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Authority shall, following the receipt of a valid VAT invoice, pay to the Contractor a sum equal to the VAT chargeable in respect of the Services.

5.5 If there is a dispute between the Parties as to the amount invoiced, the Authority shall pay the undisputed amount. The Contractor shall not suspend the supply of the Services unless the Contractor is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.

5.6 If a payment of an undisputed amount is not made by the Authority by the due date, then the Authority shall pay the Contractor interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.

5.7 If any sum of money is recoverable from or payable by the Contractor under the Agreement (including any sum which the Contractor is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Contractor under the Agreement or under any other agreement or contract with the Authority. The Contractor shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

5.8 Where the Contractor enters into a sub-contract in relation to the Services, the Contractor shall include in that sub-contract:

5.8.1 Provisions having the same effect as clauses 5.2 to 5.6 of the Agreement and

5.8.2 Provisions requiring the counterparty to that subcontract to include in any sub-contract which it awards provisions having the same effect as clauses 5.2 to 5.6 of this Agreement

5.8.3 In this clause 5.8 'sub-contract' means a contract between two or more suppliers, at any stage of remoteness from the Authority in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Agreement.

6 Premises and equipment

6.1 If necessary, the Authority shall provide the Contractor with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Authority's premises by the Contractor or the Staff shall be at the Contractor's risk.

6.2 If the Contractor supplies all or any of the Services at or from the Authority's premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Contractor shall vacate the Authority's premises, remove the Contractor's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Authority's premises in a clean, safe and tidy condition. The Contractor shall be solely responsible for making good any damage to the Authority's premises or any objects contained on the Authority's premises which is caused by the Contractor or any Staff, other than fair wear and tear.

6.3 If the Contractor supplies all or any of the Services at or from its premises or the premises of a third party, the Authority may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.

6.4 The Authority shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Authority's premises the Contractor shall, and shall procure that all Staff shall, comply with all the Authority's security requirements.

6.5 Where all or any of the Services are supplied from the Contractor's premises, the Contractor shall, at its own cost, comply with all security requirements specified by the Authority in writing.

6.6 Without prejudice to clause 3.2.6, any equipment provided by the Authority for the purposes of the Agreement shall remain the property of the Authority and shall be used by the Contractor and the Staff only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Authority on expiry or termination of the Agreement.

6.7 The Contractor shall reimburse the Authority for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Contractor or any Staff. Equipment supplied by the Authority shall be deemed to be in a good condition when received by the Contractor or relevant Staff unless the Authority is notified otherwise in writing within 5 Working Days.

6.8 Any premises/land made available from time to time to the Contractor by the Authority in connection with the contract, shall be made available to the contractor on a non-exclusive licence basis free of charge and shall be used by the contractor solely for the purpose of performing its obligations under the contract. The Contractor shall have the use of such Premises/land as licensee and shall vacate the same on completion, termination or abandonment of the Contract.

6.9 The Parties agree that there is no intention on the part of the Authority to create a tenancy of any nature whatsoever in favour of the Contractor or its Staff and that no such tenancy has of shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Authority retains the right at any time to use any premises owned or occupied by it in any manner it sees fit.

6.10 Should the Contractor require modifications to the premises of the Authority, such modifications shall be subject to prior Approval and shall be carried out by the Authority at the Contractor's expense. The Authority shall undertake approved modification work without undue delay. Ownership of such modifications shall rest with the Authority.

6.11 All the Contractor's equipment shall remain at the sole risk and responsibility of the Contractor, except that the Authority shall be liable for loss of or damage to any of the Contractor's property located on Authority's premises which is due to the negligent act or omission of the Authority.

7 Staff and Key Personnel

7.1 If the Authority reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Contractor:

7.1.1 refuse admission to the relevant person(s) to the Authority's premises;

7.1.2 direct the Contractor to end the involvement in the provision of the Services of the relevant person(s); and/or

7.1.3 require that the Contractor replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Authority to the person removed is surrendered,

and the Contractor shall comply with any such notice.

7.2 The Contractor shall:

7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures; and if requested, comply with the Authority's Staff Vetting Procedures as supplied from time to time;

7.2.2 if requested, provide the Authority with a list of the names of all persons who may require admission to the Authority's premises in connection with the Agreement;

7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Authority and provided in advance; and

7.2.4 shall at all times comply with the Supplier Code of Conduct (https://www.gov.uk/government/publications/supplier-code-of-conduct).

7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Authority, except by reason of long-term sickness, maternity leave, paternity leave, and termination of employment or other extenuating circumstances.

7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Authority (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

7.5 At the Authority's written request, the Contractor shall provide a list of names of all persons who may require admission in connection with the Contract to the Premises, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Authority may reasonably request.

7.6 The Contractor's Staff, engaged within the boundaries of the Authority's premises shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when at or outside the Authority's premises.

8 Assignment and sub-contracting

8.1 The Contractor shall not without the written consent of the Authority assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement. The Authority may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Contractor shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.

8.2 If the Contractor enters into a sub-contract for the purpose of performing its obligations under the Agreement, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Contractor to the sub-contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.

8.3 If the Authority has consented to the placing of sub-contracts, the Contractor shall, at the request of the Authority, send copies of each sub-contract, to the Authority as soon as is reasonably practicable.

8.4 The Authority may assign, novate, or otherwise dispose of its rights and obligations under the Agreement without the consent of the Contractor provided that such assignment, novation or disposal shall not increase the burden of the Contractor's obligations under the Agreement.

9 Intellectual Property Rights

9.1 All intellectual property rights in any materials provided by the Authority to the Contractor for the purposes of this Agreement shall remain the property of the Authority but the Authority hereby grants the Contractor a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Contractor to perform its obligations under the Agreement.

9.2 All intellectual property rights in any materials owned by the Contractor prior to the date of this Agreement shall remain the property of the Contractor.

9.3 All intellectual property rights in any materials created or developed by the Contractor pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Authority. If, and to the extent, that any intellectual property rights in such materials vest in the Contractor by operation of law, the Contractor hereby assigns to the Authority by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).

~~9.5~~9.4 The Contractor hereby grants the Authority a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

a) any intellectual property rights vested in or licensed to the Contractor on the date of the Agreement; and

b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which is necessary in order for the Authority to exercise its rights and take the benefit of the Agreement including the Services provided.

~~9.6~~9.5 The Contractor shall indemnify, and keep indemnified, the Authority in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by the Authority as a result of or in connection with any claim made against the Authority for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Contractor its Staff, agents or sub-contractors.

~~9.7~~9.6 The Authority shall promptly notify the Contractor of any infringement claim made against it relating to any Services and, subject to any statutory obligation requiring the Authority to respond, shall permit the Contractor to have the right, at its sole discretion to assume, defend, settle or otherwise dispose of such claim. The Authority shall give the Contractor such assistance as it may reasonably require to dispose of the claim and shall not make any statement which might be prejudicial to the settlement or defence of the claim.

10 Governance and Records

10.1 The Contractor shall:

10.1.1 attend progress meetings with the Authority at the frequency and times reasonably specified by the Authority and shall ensure that its representatives are suitably qualified to attend such meetings; and

10.1.2 submit progress reports to the Authority at the times and in the format specified by the Authority.

10.2 The Contractor shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Authority. The Contractor shall on request afford the Authority or the Authority's representatives such access to those records as may be reasonably requested by the Authority in connection with the Agreement.

11 Confidentiality, Transparency and Publicity

11.1 Subject to clause 11.2, each Party shall:

11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:

11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

11.2.2 to its auditors or for the purposes of regulatory requirements;

11.2.3 on a confidential basis, to its professional advisers;

11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;

11.2.5 where the receiving Party is the Contractor, to the Staff, agents, or sub-contractors on a need to know basis to enable performance of the Contractor's obligations under the Agreement provided that the Contractor shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Contractor's confidentiality obligations under the Agreement;

11.2.6 in accordance with clause 12; and

11.2.7 where the receiving Party is the Authority:

a) on a confidential basis to the employees, agents, consultants and contractors of the Authority;

b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Authority transfers or proposes to transfer all or any part of its business; or

c) to the extent that the Authority (acting reasonably) deems disclosure necessary in the course of carrying out its public functions; or

d) in accordance with clause 12.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this clause 11.

11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Contractor hereby gives its consent for the Authority to publish this Agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Authority may consult with the Contractor to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

11.4 The Contractor shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Authority.

12 Freedom of Information

12.1 The Contractor acknowledges that the Authority is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall procure that any sub-contractor shall:

12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;

12.1.2 transfer to the Authority all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 Working Days of receipt;

12.1.3 provide the Authority with a copy of all Information belonging to the Authority requested in the Request for Information which is in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may reasonably specify) of the Authority's request for such Information; and

12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Authority.

12.2 The Contractor acknowledges that the Authority may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Contractor or the Services (including commercially sensitive information) without consulting or obtaining consent from the Contractor. In these circumstances the Authority shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Contractor advance notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.

12.3 Notwithstanding any other provision in the Agreement, the Authority shall be responsible for determining in its absolute discretion whether any Information relating to the Contractor or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

12.4 Where the Parties are both subject to the requirements of the FOIA, the obligations in this clause 12 shall equally apply to each Party.

13 Protection of Personal Data and Security of Data

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

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

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

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

(a) process that Personal Data only in accordance with Schedule 4, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event,, having taken account of the:

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

(c) ensure that:

(i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 4);
(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

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

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer

(whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

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

13.5 Subject to clause 13.6, the Processor shall notify the Controller immediately if, in relation to this Contract, it:

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

13.6 The Processor's obligation to notify under clause 13.5 shall include the provision of further information to the Controller in phases, as details become available.

13.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 13.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;
(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
(d) assistance as requested by the Controller following any Data Loss Event;

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

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

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

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

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

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

(a) notify the Controller in writing of the intended Sub-processor and processing;
(b) obtain the written consent of the Controller;
(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 13 such that they apply to the Sub-processor; and
(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

13.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

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

13.14 Subject to clause 14.5, the Processor shall indemnify the Controller on a continuing basis against any and all Losses incurred by the Controller arising from the Processor's Default under this clause 13 and/or any failure by the Processor or any Sub-processor to comply with their respective obligations under Data Protection Legislation.

13.15 Nothing in this clause 13 shall be construed as requiring the Processor or any relevant Sub-processor to be in breach of any Data Protection Legislation.

13.16 The provision of this clause 13 applies during the Term and indefinitely after its expiry.

13A Security

13A.1 The Authority shall be responsible for maintaining the security of the Authority's premises in accordance with its standard security requirements. The Contractor shall comply with all security requirements of the Authority while on the Authority's premises, and shall ensure that all Staff comply with such requirements.

13A.2 The Contractor shall ensure that any Security Plan produced by the Contractor fully complies with the Security Policy.

13A.3 The Contractor shall comply, and shall procure compliance of its Staff, with the Security Plan and Security Policy.

13A.4 The Authority shall notify the Contractor of any changes or proposed changes to the Security Policy.

13A.5 The Contractor shall, as an enduring obligation during the Contract Period, use the latest versions of anti-virus definitions available from an industry accepted anti-virus software vendor to check for and delete Malicious Software from the ICT Environment.

13A.6 Notwithstanding clause 13A.5, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of the Authority Data, assist each other to mitigate any losses and to restore the provision of Services to their desired operating efficiency and the Contractor shall immediately take all reasonable steps necessary to:

(a) minimise the extent of actual or potential harm caused by any Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure; and

(d) as soon as reasonably practicable provide the Authority with full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority.

13A.7 Any cost arising out of the actions of the Parties taken in compliance with clause 13A.6 shall be borne by the Parties as follows:

(a) by the Contractor where the Malicious Software originates from the Contractor Software, the Third Party Software or the Authority Data (whilst the Authority Data was under the control of the Contractor); and

(b) by the Authority if the Malicious Software originates from the Authority's Software or Authority Data (whilst the Authority Data was under the control of the Authority).

13A.8 The Contractor controlled architecture and environment used to process or store Authority Data will be certified to the NCSC Cyber Essentials Plus certification scheme.

13A.9 Subject to clause 14.5, the Contractor shall be liable for, and shall indemnify the Authority against all Losses suffered or incurred by the Authority and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of Security (to the extent that such Losses were not caused by any act or omission by the Authority).

14 Liability and Insurance

14.1 The Contractor shall not be responsible for any injury, loss, damage, cost or expense suffered by the Authority if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under the Agreement.

14.2 Subject always to clauses 14.3 and 14.4:

14.2.1 the aggregate liability of the Contractor in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed 125% of the Charges paid or payable to the Contractor; and

14.2.2 except in the case of claims arising under clauses 9.5 and 18.4, in no event shall the Contractor be liable to the Authority for any:

a) loss of profits;

b) loss of business;

c) loss of revenue;

d) loss of or damage to goodwill;

e) loss of savings (whether anticipated or otherwise); and/or

f) any indirect, special or consequential loss or damage.

14.3 Nothing in the Agreement shall be construed to limit or exclude either Party's liability for:

14.3.1 death or personal injury caused by its negligence or that of its Staff;

14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or

14.3.3 any other matter which, by law, may not be excluded or limited.

14.4 The Contractor's liability for all Losses suffered or incurred by the Authority arising from the Contractor's Default resulting in the destruction, corruption, degradation or damage to Authority Data or any copy of such Authority Data shall in no event exceed £10,000,000.

14.5 The Contractor shall hold:

a) Employer's liability insurance providing an adequate level of cover in respect of all risks which may be incurred by the Contractor;

b) Public liability with the minimum cover per claim of one million pounds (£1,000,000);

c) Professional indemnity with the minimum cover per claim of £ one million pounds (£1,000,000);

or any sum as required by Law unless otherwise agreed with the Authority in writing. Such insurance shall be maintained for the duration of the Term and for a minimum of six (6) years following the expiration or earlier termination of the Agreement.

15 Force Majeure

15.1 Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Contractor. Each Party shall promptly notify the other Party in writing, using the most expeditious method of delivery, when such circumstances cause a delay or failure in performance, an estimate of the length of time delay or failure shall continue and when such circumstances cease to cause delay or failure in performance. If such circumstances continue for a continuous period of more than 30 days, either Party may terminate the Agreement by written notice to the other Party.

15.2 Any failure by the Contractor in performing its obligations under the Agreement which results from any failure or delay by an agent, sub-contractor or supplier shall be regarded as due to Force Majeure only if that agent, sub-contractor or supplier is

itself impeded by Force Majeure from complying with an obligation to the Contractor.

16 Termination

16.1 The Authority may terminate the Agreement at any time by notice in writing to the Contractor to take effect on any date falling at least 3 months (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.

16.2 Without prejudice to any other right or remedy it might have, the Authority may terminate the Agreement by written notice to the Contractor with immediate effect if the Contractor:

16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;

16.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;

16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Contractor receiving notice specifying the breach and requiring it to be remedied;

16.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;

16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13 and 17, 18, 20; or

16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Contractor (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Contractor's assets or business, or if the Contractor makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction.

16.3 The Contractor shall notify the Authority as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.

16.4 The Contractor may terminate the Agreement by written notice to the Authority if the Authority has not paid any undisputed amounts within 60 days of them falling due.

16.5 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 13A, 14, 16.6, 17.4, 18.4, 19 and 20.8 or any other provision of the Agreement that either expressly or by implication has effect after termination.

16.6 Upon termination or expiry of the Agreement, the Contractor shall:

16.6.1 give all reasonable assistance to the Authority and any incoming Contractor of the Services to the extent necessary to effect an orderly assumption by a Replacement Contractor in accordance with the procedure set out in Schedule 8 – Exit Management Strategy; and

16.6.2 return all requested documents, information and data to the Authority as soon as reasonably practicable.

17 Compliance

17.1 The Contractor shall promptly notify the Authority of any health and safety hazards which may arise in connection with the performance of its obligations under the Agreement. The Authority shall promptly notify the Contractor of any health and safety hazards which may exist or arise at the Authority's premises and which may affect the Contractor in the performance of its obligations under the Agreement.

17.2 The Contractor shall:

17.2.1 comply with all the Authority's health and safety measures while on the Authority's premises; and

17.2.2 notify the Authority immediately of any incident occurring in the performance of its obligations under the Agreement on the Authority's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

17.3 The Contractor shall:

17.3.1 perform its obligations under the Agreement in accordance with all applicable equality Law and the Authority's equality and diversity policy; and

17.3.2 take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.

17.4 The Contractor shall supply the Services in accordance with the Authority's environmental policy as provided to the Contractor in advance.

18 Prevention of Fraud, Corruption and Bribery

18.1 The Contractor represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:

18.1.1 Committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act and/or

18.1.2 Been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

18.2 The Contractor shall not during the Term:

18.2.1 commit a Prohibited Act; and/or

18.2.2 do or suffer anything to be done which would cause the Authority or any of its employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

18.3 The Contractor shall, during the Term establish, maintain and enforce, and require that its Sub-Contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act; and shall notify the Authority immediately if it has reason to suspect that any breach of clauses 18.1 and/or 18.2 has occurred or is occurring or is likely to occur.

18.4 If the Contractor or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Authority) the Authority may:

18.4.1 terminate the Agreement and recover from the Contractor the amount of any loss suffered by the Authority resulting from the termination, including the cost reasonably incurred by the Authority of making other arrangements for the supply of the Services and any additional expenditure incurred by the Authority throughout the remainder of the Agreement; or

18.4.2 recover in full from the Contractor any other loss sustained by the Authority in consequence of any breach of this clause.

19 Dispute Resolution

19.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.

19.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the "Mediator") chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.

19.3 If the Parties fail to appoint a Mediator within one month 20 Working Days of the agreement to refer to a Mediator, either Party shall apply to the Centre for Effective Dispute Resolution to appoint a Mediator.

19.4 If the Parties fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, or such longer period as may be agreed by the Parties, either Party may refer the dispute to Court.

19.5 The commencement of mediation shall not prevent the parties commencing or continuing court or arbitration proceedings in relation to the dispute.

20 General

20.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.

20.2 A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties. This clause does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999 and does not apply to the Crown.

20.3 Subject to Clause 3.4, the Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.

20.4 In the event that the Contractor is unable to accept the Variation to the Specification or where the Parties are unable to agree a change to the Contract Price, the Authority may:

20.4.1 allow the Contractor to fulfil its obligations under the Agreement without the Variation to the Specification;

20.4.2 terminate the Contract with immediate effect, except where the Contractor has already provided all or part of the Services or where the Contractor can show evidence of substantial work being carried out to fulfil the requirement of the Specification, and in such case the Parties shall attempt to agree upon a resolution to the matter. Such termination or expiry shall be without prejudice to the right of either Party to recover any amount outstanding at such termination or expiry. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at clause 19.

20.5 The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.

20.6 Any waiver or relaxation by either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.

20.7 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.

20.8 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

20.9 If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.

20.10 The Contractor shall take appropriate steps to ensure that neither the Contractor nor any Staff is placed in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Contractor and the duties owed to the Authority under the provisions of the Agreement. The Contractor will disclose to the Authority full particulars of any such conflict of interest which may arise.

20.11 The Authority reserves the right to terminate the Agreement immediately by notice in writing and/or to take such other steps it deems necessary where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or potential conflict between the pecuniary or personal interest of the Contractor and the duties owed to the Authority pursuant to this clause shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

20.12 The Agreement constitutes the entire contract between the Parties in respect of the matters dealt with therein. The Agreement supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause shall not exclude liability in respect of any Fraud or fraudulent misrepresentation.

21 Notices

21.1 Except as otherwise expressly provided in the Agreement, no notice or other communication from one Party to the other shall have any validity under the Agreement unless made in writing by or on behalf of the Party concerned.

21.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter (sent by hand, first class post, recorded delivery or special delivery), or by facsimile transmission or electronic mail (confirmed in either case by letter), Such letters shall be addressed to the other Party in the manner referred to in clause 21.3. Provided the relevant communication is not returned as undelivered, the notice or communication shall be deemed to have been given 2 Working Days after the day on which the letter was posted, or 4 hours, in the case of electronic mail or facsimile transmission or sooner where the other Party acknowledges receipt of such letters, facsimile transmission or item of electronic mail.

21.3 For the purposes of clause 21.2, the address of each Party shall be:

21.3.1 For the Authority: Care Quality Commission

[Address:] 151 Buckingham Palace Road

London

IN WITNESS of which this Agreement has been duly executed by the parties on the date first above written.

SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Signature [redacted]

Name ...

Position ...

SIGNED for and on behalf of **UNIVERSITY OF PLYMOUTH ENTERPRISE LIMITED**

Signature ..... [redacted]

Name .....

Position .....

SCHEDULE 1 – INVITATION TO TENDER AND SPECIFICATION

1. Background

Healthwatch England is seeking to commission an organisation to undertake a review of literature and research to help inform our work to promote effective public engagement in health and social care. Healthwatch England has identified that while the existence of legal requirements for those who design and deliver services to engage with those who use services is generally well understood, the real and tangible benefits of that engagement for those who design, provide, fund and use services is often less well understood and less easily demonstrable.

We are seeking to enable Healthwatch and our local and national partners to better make the case for effective engagement activity at a time when services are in the process of being re-designed to an unprecedented level and when people's engagement with that process is more important than ever.

This literature review will provide a basis for subsequent work by Healthwatch England to:

- Provide context for the current legislative framework for engagement;
- Describe engagement in its various forms and, focussing on outcomes, identify the benefits associated with differing methodologies;
- Identify other factors influencing the outcomes of engagement and its impact;
- Quantify the outcomes of engagement (developing a framework), so the cost benefits and the cost of not engaging, or engaging ineffectively, can be calculated;
- Investigate the value of a co-ordinated approach to engagement across health and social care;
- Use and test the above framework to demonstrate the outcomes of local Healthwatch engagement activity.

It is therefore a critical first step for us to identify and understand the research and evidence that already exists.

1.1 Healthwatch

We are the independent champion for people who use health and social care services in England. We exist to make sure that people are at the heart of care. We listen to what people like about services and what could be improved. We share their views with those with the power to make change happen. We also help people find the information they need about services in their area.

We have the power to make sure that people's voices are heard by the government and those running services. As well as seeking the public's views ourselves, we also encourage services to involve people in decisions that affect them. Our sole purpose is to help make care better for people.

In summary – Healthwatch is here to:

- Help people find out about local care
- Listen to what people think of services
- Help improve the quality of services by letting those running services and the government know what people want from care
- Encourage people running services to involve people in changes in care

1.2 The Requirement

We require a review of literature and research that delivers the following outcomes:

- Identify robust research that has been undertaken to understand approaches to, and the impact, effectiveness and cost-effectiveness of, public and community engagement in publicly commissioned health and social care services, in the UK and elsewhere.
- Identify existing research findings concerning the experiences of individuals, communities and organisations in relation to these public engagement activities and their outcomes.
- Identify non-research evidence from other relevant academic or sectoral publications and secondary sources.
- Identify relevant legal cases and judgments in England.
- Identify evidence relating to engagement in the development and implementation of Sustainability and Transformation Plans/Partnerships and Accountable Care
- Identify any evidence concerning differential levels of engagement in relation to different social groups, considering the protected characteristics covered by the Equality Act and other relevant demographics.

Evidence concerning engagement to influence service improvement and engagement and consultation in relation to service change and transformation are both in scope for this project.

Indicative timeline:

Phase one – Project planning and final agreement of research parameters (Week 3/4, July 2018)

- **Agree timeframes for delivery**
- **Agree format for delivery**
- **Agree SMART scope**

Phase two – Undertake literature review (August-mid September 2018)

Phase three – Present final product (end September 2018)

Outputs
To be finalised in agreement with the commissioned organisation but could contain:

- A briefing with a clear executive summary;
- A slide pack summarising the findings;
- A clear bibliography with links to research;
- Links and references to useful case studies.

1.3 Contact and reporting

At the contract start, a set-up meeting will be held to agree project methodology and timeline, including key reporting milestones. Throughout the project, Healthwatch England will require a weekly progress update.

1.4 Roles and responsibilities

The overall project sponsor and your point of contact will be [redacted] Healthwatch England).

SCHEDULE 2 – CHARGES

The total cost of the research will be **£19,221.64 plus VAT**. Table one below provides an itemised breakdown of these costs. Please note that this proposal factors in travel for two SERIO team members to attend meetings, one at the outset and a final presentation meeting. There is potential for savings to be made by conducting these meeting remotely, should Healthwatch wish to do so, however we recommend that we allow this time in order to fully meet the needs of Healthwatch.

Table 1: Breakdown of Review Costs

	Alice Hocking Head of SERIO	Pamela Varley Research Manager, SERIO	Donna Vascott Researcher, SERIO	Claudia Blandon Research Assistant, SERIO	Total
Project management		[redacted]			
Inception meeting					
Develop and refine search strategy					
Screen and select for inclusion					
Extract and synthesize results					
Call for evidence					
Reporting					
Final meeting					
Total Number of Days					
Day Rate					
Total Staff Costs					
Travel and Subsistence					
Total Costs					£19,221.64 plus VAT

Frequency of Invoicing

In accordance with clause 5.2, the Contractor shall invoice the Authority on completion of the Services. Payment will be made after completion of the Contract and not in stages.

SCHEDULE 3 – TENDER RESPONSE

UNDERSTANDING THE ISSUE

Patient and public involvement is now at the forefront of the UK policy agenda, enshrined in legislation, and expected to be a core consideration in both the design and delivery of health and social care services. Despite the championing of more holistic measures that place patient experience and engagement at the core, debate continues regarding the way in which patients and the public can be *effectively* engaged, and the means by which this should be carried out. Healthwatch England require a review of literature and research relating to public engagement in both service improvement and service transformation, focussing particularly on the outcomes and effectiveness of engagement across the fields of health and social care. The specification calls for outputs that can guide next steps, and enable Healthwatch to develop a case for effective engagement activity by addressing the following key questions:

- What works with respect to public engagement in health and social care services?
- What contributes to best practice?
- What is the lasting impact of effective engagement?
- What are the quantitative and qualitative benefits of differing approaches?
- What factors are at play in engagement outcomes?
- What social stratification exists within public engagement activities?

To this end, SERIO has designed a robust research approach that is clear, transparent and methodical. Resultant outputs will ensure Healthwatch gain an advanced understanding of the breadth of existing research and evidence, and can be utilised to inform subsequent decision-making.

2. WHO WE ARE

SERIO, an applied research unit based at the University of Plymouth, is uniquely placed to successfully deliver Healthwatch's brief. As a university, we have unbridled access to a wide range of academic literature sources, as well as having ongoing working relationships with a variety of library and information specialists - experts within their individual fields. We have a wealth of experience in the policy arena, including considerable sector specific health and social care expertise. This wide-reaching background sees us very well placed to make a judgement on the balance of robust, quality information, with information that is both useful and applicable. We understand, and are sensitive to, the need to produce outputs which are robust and persuasive to policy makers, but also accessible and easily utilised. SERIO has a wealth of experience of delivering literature reviews and more structured systematic reviews. A solid literature review has provided the basis of many research projects we have engaged in, often featuring as a standalone research output.

3. OUR APPROACH

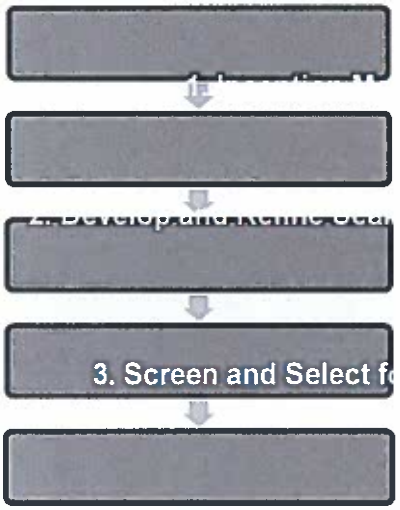
The following section sets out our chosen method, which has been designed in order to deliver on Healthwatch's specification, but also to provide value for money within budget parameters.

Given the timescale and budget, and the need to capture and condense a large number of sources, we feel a rapid evidence assessment approach is most appropriate. This approach will involve a focus on set research questions, which we will finalise with Healthwatch in advance.

METHODOLOGY

Our approach is based on our experience of delivering similar projects and aims to maximise opportunities to learn from existing knowledge and understanding on patient and public engagement. The following diagram summarises our intended approach, with further details on each stage of the process provided below.

Figure 1: Summary of SERIO's Review Approach



1. Inception Meeting

The inception meeting is a key starting point to any project, and in our experience is instrumental in ensuring good progress and communication throughout. It will allow us to discuss and agree the review methodology, finalise the project timeline and respond to any queries. We will outline in detail the intended approach and seek to tailor and refine this with input from Healthwatch in order to best meet their needs. This will also provide an opportunity to agree output delivery dates, and confirm the formats in which they will be received, as well as reach understanding on Healthwatch's vision for the final briefing report in terms of style, presentation, infographics, etc.

2. Develop and Refine Research Strategy

Following the inception meeting, SERIO will develop a search strategy, identifying an index of key search terms and any variants. We will conduct an initial broad, sensitive search in order to avoid the omission of relevant materials. Bearing in mind the scope of the review, as set out by Healthwatch in the specification, we will include a wide range of resources and databases in our search. We anticipate that many relevant documents will not be indexed in academic databases and it is important that the search strategy includes grey literature sources and legal databases to reflect this. This will optimize the retrieval of relevant materials and ensure we conduct a targeted search which captures both research and non-research items, incorporating a comprehensive blend of robust research, grey literature and legal cases. We will agree the electronic databases to be included within the search strategy with Healthwatch. However, examples of the types of databases that could be included are:

- MEDLINE (Ovid) – a premier database for searching medical and healthcare literature
- SocINDEX (EBSCO) – sociology research database
- Taylor and Francis Online - multi-disciplinary database
- Scopus - covers international research output in the fields of science, technology, medicine, social sciences, and arts and humanities
- OpenGrey - system for information on grey literature in Europe
- INVOLVE Libraries - public involvement in research
- Westlaw - covers UK legislation and a wealth of case law

The research team, as part of the University of Plymouth, will have access to all of the above, which are either subscription based or with open access. They encompass a wide range of disciplines in order to ensure the breadth of evidence required for this review is collated. Databases such as OpenGrey will assist in identifying relevant grey literature. It is anticipated that the evidence from grey literature will contribute to providing greater granularity to what works, how and why. We will also search for grey literature through general internet browsing using a pre-agreed broad set of search terms and key sites.

The search strategy will be developed as an iterative process, building upon test searches and assessments made by the team. Having developed an exhaustive list of index terms, ensuring synonyms and variants are accounted for, we will execute various combinations of these search terms, narrowing the search as appropriate in order to drill down to the most relevant and applicable literature. This review method will be adapted as appropriate to apply to the retrieval

of grey literature, legal case information and sectoral evidence, tailoring the search terms to ensure they are applicable to the relevant databases.

3. Screen and Select for Inclusion

The next stage involves a thorough review and refinement of search results, selecting and appraising results for inclusion in the final review. Criteria for the inclusion and exclusion of evidence in the review will be developed in accordance with the brief, and can be agreed with Healthwatch, following which we will engage in the cautious and gradual application of search filters. For instance, we will seek to put an appropriate time limit on the return of results and confine the geographical reach of the search to regions deemed suitable by Healthwatch (e.g. including only results which have been published post-2008, and confining the target search area to Europe). All stages of the review will employ a transparent and methodical process, which will be clearly documented.

Duplicates will be removed from the retrieved search results. Titles and abstracts will be screened by an experienced reviewer using the pre-agreed inclusion and exclusion criteria. The quality of all of the included studies (quantitative and qualitative) will be assessed by a pre-agreed quality appraisal checklist. However, given that many of the documents are likely to be unpublished and relatively small-scale research projects, we will only apply pre-existing checklists if it is appropriate to do so. Again, this approach will be adapted as appropriate to cater to evidence returned in different formats. A detailed bibliography will list all items included in the literature review, with links provided where possible. Once selected for inclusion, all sources will be saved in a secure online university repository for reference. This data store will be available to the client upon completion of the research, if required.

4. Call for Evidence

At this stage in the process, SERIO will have a clear indication of the direction of travel of the literature review. Gaps in evidence will be identifiable, and it is at this point we will seek to distribute a call for evidence. This is a notice to networks of organisations who may commission research that we are unaware of, and provides an opportunity for them to forward relevant materials to us. In our experience of this kind of work, we have found that a call for evidence can be effective in filling knowledge gaps by providing access to useful research which has been commissioned but remains unpublished. SERIO will distribute this call for evidence via appropriate channels which will be agreed with Healthwatch but may include, for example, [redacted] All evidence returned that meets set criteria and falls within a certain quality threshold will be assessed and incorporated into the review where appropriate. This call for evidence will allow for an additional avenue of enquiry, and may glean evidence which could otherwise, potentially, fail to be captured.

5. Extract and Synthesize Results

Once we have fully executed the search strategy and applied all inclusion/ exclusion criteria, we will begin the process of extracting and synthesising data. Data will be extracted from all selected items, with search results grouped based on the outcomes examined. At this stage, it will be possible to identify case studies that are particularly relevant to Healthwatch's aims. These will

be shortlisted, with a final list of those deemed most robust included in a separate appendix, along with links and a brief description of headline details.

The final stage of the review process, prior to preparation of the final briefing report, will be the synthesis of results, bringing together findings from the wide range of data sources explored over the course of the research. Academic outputs, grey literature and any additional sources will be blended, with evidence synthesised to inform robust and applicable outputs. We will collate all evidence obtained and summarise findings in a comprehensive briefing report, providing a balanced view and commentary on conclusions, policy implications and any limitations. Research outputs will make clear, according to available evidence, what works with respect to public engagement in health and social care services; what contributes to best practice; the lasting impact of effective engagement; the quantitative and qualitative benefits of differing approaches; the factors at play in engagement outcomes; and social stratification within public engagement activities. Further details on our suggested reporting outputs are detailed below.

REPORTING

By mid-September, SERIO will deliver a draft package of research outputs which can be readily used to develop a case with respect to public engagement. Details of suggested individual components are outlined below, to be agreed upon at the inception meeting in July.

SERIO will provide an overarching final briefing report, which will interpret results and situate them within the context of Healthwatch's agenda, as well as commenting on any limitations identified and the implications for future research. It will be accompanied by a clear, concise executive summary, which highlights key findings and condenses results into an easily digestible and relatable format. In addition, we will provide a comprehensive bibliography, including links to sources used where possible. All literature and research collated for this review will be saved within a secure online repository, and will be available for client access upon completion of the research if required. A further appendix will provide specifics on noteworthy case studies which will be of particular interest to Healthwatch, including links to these studies and a concise summary of their highlights. The report and appendices outlined above will be accompanied by a PowerPoint slide presentation which summarises key findings in a visually engaging manner. SERIO can deliver this presentation at the final meeting and will invite discussion with Healthwatch on the implications of the review and next steps. A summary of our suggested research outputs is listed below, all of which will be delivered in draft format by mid-September, with comments invited before production of revised, final versions by the end of September:

- **Overarching final briefing report**
- **Concise executive summary**
- **Appendix of noteworthy case studies**

- **Comprehensive bibliography**
- **PowerPoint Slide Presentation**

PROJECT MANAGEMENT

Following the inception meeting, when the project is up and running, SERIO will provide an update to Healthwatch England at the end of each working week for the duration of the project. This will outline progress towards agreed objectives; detail next steps for the coming week; give an indication of the direction of travel of the research results; and agree solutions for any challenges identified as the review develops. Weekly project catch-ups can take place via a diarised telephone call or be delivered by email, depending on Healthwatch's particular preference.

We have also allocated time for attendance at a final meeting with Healthwatch, in order to deliver a final presentation on the research findings and discuss outcomes and implications.

4. TRACK RECORD

[redacted]

5. THE REVIEW TEAM

Our team for this assignment is detailed below. In addition, we have full access to information specialists at the University who have specialist knowledge in conducting reviews.

[redacted]

[redacted]

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS – NOT USED

1. The Contractor shall comply with any further written instructions with respect to processing by the Authority.

2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	
Type of personal data	
Categories of Data Subject	
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	

SCHEDULE 5 – SECURITY REQUIREMENTS, POLICY AND PLAN

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 5, unless the context otherwise requires the following provisions shall have the meanings given to them below:

"Breach of Security" means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor system, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.

"Contractor Equipment" means the hardware, computer and telecoms devices and equipment supplied by the Contractor or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

"Contractor Software" means 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 and which is specified as such in Schedule 7.

"ICT" means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

"Good Industry Practice" the standards which fall within the upper quartile in the relevant industry for the provision of comparable services which are substantially similar to the Services or the relevant part of them, having regard to factors such as the nature and size of the parties, the KPIs, the term, the pricing structure and any other relevant factors.

"Protectively Marked" shall have the meaning as set out in the Security Policy Framework.

"Security Plan" means the Contractor's security plan prepared pursuant to paragraph 3 an outline of which is set out in an Appendix to this Schedule 5.
"Software" means Specially Written Software, Contractor Software and Third Party Software.

"Specially Written Software" means any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this Contract.

"Third Party Software" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software and which is specified as such in Schedule 7.

1. INTRODUCTION

This Schedule 5 covers:

1.1 principles of security for the Contractor system, derived from the Security Policy Framework, including without limitation principles of physical and information security;

1.2 wider aspects of security relating to the Services;

1.3 the creation of the Security Plan;

1.4 audit and testing of the Security Plan; and

1.5 breaches of security.

2. PRINCIPLES OF SECURITY

2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.

2.2 The Contractor shall be responsible for the security of the Contractor system and shall at all times provide a level of security which:

2.2.1 is in accordance with Good Industry Practice and Law;

2.2.2 complies with Security Policy Framework; and

2.2.3 meets any specific security threats to the Contractor system.

2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):

2.3.1 loss of integrity of Authority Data;

2.3.2 loss of confidentiality of Authority Data;

2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;

2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;

2.3.5 use of the Contractor system or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and

2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.

2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule 5.

3.2 A draft Security Plan provided by the Contractor as part of its bid is set out herein.

3.3 Prior to the Commencement Date the Contractor will deliver to the Authority for approval the final Security Plan which will be based on the draft Security Plan set out herein.

3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause I2 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.4 shall be deemed to be reasonable.

3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

3.5.1 the provisions of this Schedule 5;

3.5.2 the provisions of Schedule 1 relating to security;

3.5.3 the Information Assurance Standards;

3.5.4 the data protection compliance guidance produced by the Authority;

3.5.5 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;

3.5.6 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and

3.5.7 appropriate ICT standards for technical countermeasures which are included in the Contractor system.

3.6 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.

3.7 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary to other schedules of the Contract which cover specific areas included within that standard.

3.9 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 5.

4. AMENDMENT AND REVISION

4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:

4.1.1 emerging changes in Good Industry Practice;

4.1.2 any change or proposed change to the Contractor system, the Services and/or associated processes;

4.1.3 any new perceived or changed threats to the Contractor system;

4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or

4.1.5 a reasonable request by the Authority.

4.2 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of an Authority request or change to Schedule 1 or otherwise) shall be subject to a Change Control Notice and shall not be implemented until Approved.

5. AUDIT AND TESTING

5.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

5.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in an Approved form) as soon as practicable after completion of each Security Test.

5.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services.

5.4 Where any Security Test carried out pursuant to paragraphs 5.2 or 5.3 reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to Approval in accordance with paragraph 4.3, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy Framework or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

6. BREACH OF SECURITY

6.1 Either Party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall immediately take all reasonable steps necessary to:

6.2.1 remedy such breach or protect the Contractor system against any such potential or attempted breach or threat; and

6.2.2 prevent an equivalent breach in the future;

6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;

6.2.4 investigate the incident and produce a detailed report for the Authority within 5 working days of the discovery of the incident.

6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the CCN procedure set out in Schedule 4.

6.4 The Contractor shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

7. CONTRACT EXIT – SECURITY REQUIREMENTS

7.1 In accordance with clause H7 of the Contract, on termination of the Contract, either via early termination or completion of the Contract then the Contractor will either return all data to the Authority or provide a certificate of secure destruction using an industry and Authority approved method. Destruction or return of the data will be specified by the Authority at the time of termination of the Contract.

APPENDIX 1- OUTLINE SECURITY PLAN

ANNEX 1: BASELINE SECURITY REQUIREMENTS

1. HIGHER CLASSIFICATIONS

1.1 The Contractor shall not handle Authority Data and information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Contractor shall seek additional specific guidance from the Authority.

2. END USER DEVICES

2.1 When Authority Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Authority Data and services must be under the management authority of the Authority or Contractor and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Authority. Unless otherwise agreed with the Authority in writing, all Contractor devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2). Where the guidance highlights shortcomings in a particular platform the Contractor may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. Where the Contractor wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Authority.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

3.1 The Contractor and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Contractor must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.

3.2 The Contractor shall agree any change in location of data storage, processing and administration with the Authority in advance where the proposed location is outside the UK. Such approval shall not be unreasonably withheld or delayed unless specified otherwise in this Agreement and provided that storage, processing and management of any Authority Data are only carried out offshore within:

3.2.1 the European Economic Area (EEA);

3.2.2 in the US if the Contractor and or any relevant Sub-Contractor have signed up to the US-EU Privacy Shield Register; or

3.2.3 in another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its

domestic law or of the international commitments it has entered into which have been defined as adequate by the EU Commission.

3.3 The Contractor shall:

3.3.1 provide the Authority with all Authority Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Authority Data in the event of the Contractor ceasing to trade;

3.3.3 securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Authority Data held by the Contractor when requested to do so by the Authority.

4. NETWORKING

4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

4.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY ARCHITECTURES

5.1 The Contractor shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Authority Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) the Contractor shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification(http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor).

6. PERSONNEL SECURITY

6.1 Contractor Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Contractor shall agree on a case by case basis Contractor Personnel roles which require specific government clearances (such as 'SC') including system

administrators with privileged access to IT systems which store or process Authority Data.

6.3 The Contractor shall prevent Contractor Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Authority Data except where agreed with the Authority in writing.

6.4 All Contractor Personnel that have the ability to access Authority Data or systems holding Authority Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Authority in writing, this training must be undertaken annually.

6.5 Where the Contractor or Sub-Contractors grants increased ICT privileges or access rights to Contractor Personnel, those Contractor Personnel shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. IDENTITY, AUTHENTICATION AND ACCESS CONTROL

7.1 The Contractor shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Contractor shall retain an audit record of accesses.

8. AUDIT AND MONITORING

8.1 The Contractor shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Contractor shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 months.

ANNEX 2: SECURITY POLICY

CQC Security Policy can be found on CQC website

ANNEX 3: SECURITY MANAGEMENT PLAN – NOT USED

SCHEDULE 6 – CHANGE CONTROL

Contract Change Note

Contract Change Note Number **Contract Reference Number & Title** **Variation Title** **Number of Pages**	

WHEREAS the Contractor and the Authority entered into a Contract for the supply of [project name] dated [dd/mm/yyyy] (the "Original Contract") and now wish to amend the Original Contract

IT IS AGREED as follows

1. The Original Contract shall be amended as set out in this Change Control Notice:

Change Requestor / Originator		
Summary of Change		
Reason for Change		
Revised Contract Price	Original Contract Value	£
	Previous Contract Changes DN: Enter all CCN's here so that total value is shown for Audit purposes	£
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details) DN: Any change to Specification should be added as an Annex to the CCN		
Revised Contract Period		
Change in Contract Manager(s)		
Other Changes		

2. Save as herein amended all other terms of the Original Contract shall remain effective.

3. This Change Control Notice shall take effect from the date on which both the Authority and the Contractor have communicated acceptance of its terms.

SIGNED ON BEHALF OF THE AUTHORITY:	SIGNED ON BEHALF OF THE CONTRACTOR:
Signature:	Signature:
Name:	Name:
Position:	Position:
Date:	Date:

SCHEDULE 7 – THIRD PARTY SOFTWARE – NOT USED

CONTRACTOR SOFTWARE

For the purposes of this Schedule 7, "**Contractor Software**" means 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. The Contractor Software comprises the following items:

Software	Supplier (if Affiliate of the Contractor)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

THIRD PARTY SOFTWARE

For the purposes of this Schedule 7, "**Third Party Software**" means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software specified in this Schedule 7. The Third Party Software shall consist of the following items:

Third Party Software	Supplier	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY – NOT USED