CareQuality Commission

www.cqc.org.uk

Contract (Short Form – Services)

Contract for the provision of Public Research

Contract Reference CQC PSO 204

November 2019

Contents

1 Interpretation 2

2 Priority of documents 6

3 Supply of Services 7

4 Term 7

5 Charges, Payment and Recovery of Sums Due 8

6 Premises and equipment 9

7 Staff and Key Personnel 10

8 Assignment and sub-contracting 11

9 Intellectual Property Rights 12

10 Governance and Records 13

11 Confidentiality, Transparency and Publicity 13

12 Freedom of Information 14

13 Protection of Personal Data 15

13A Security 18

14 Liability and Insurance 19

15 Force Majeure 20

16 Termination 20

17 Compliance 22

18 Prevention of Fraud, Corruption and Bribery 22

19 Dispute Resolution 23

20 General 24

21 Notices 25

22 Governing Law and Jurisdiction 26

23 TUPE – NOT APPLICABLE 26

SCHEDULE 1 – INVITATION TO TENDER AND SPECIFICATION 28

SCHEDULE 2 – CHARGES 37

SCHEDULE 3 – TENDER RESPONSE 42

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS 51

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN 55

SCHEDULE 6 – CHANGE CONTROL 76

SCHEDULE 7 – THIRD PARTY SOFTWARE 77

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY 78

THIS CONTRACT is dated 1st of November 2019

PARTIES

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

and

(2) **Office for Public Management Ltd trading as Traverse** of 252B Gray's Inn Road, London, WC1X 8XG, Company number: 2343617 (**"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. In order of the provision of Public Research.
3. The Contractor has been appointed by the Authority to provide the Services.
4. 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:

"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;
"Award Letter"	means the letter from the Authority to the Contractor containing these terms and conditions;
"Anti-Slavery and Human Trafficking Laws"	means all applicable anti-slavery and human trafficking laws, statutes, regulations, policies and codes from time to time in force including but not limited to the Modern Slavery Act 2015;
"Breach of Security"	means any incident that result in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms;
"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;
"Contract"	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 the Authority the Contractor;
"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;
"Contractor"	means the person named as Contractor who was awarded this contract;
"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 [subject to Royal Assent] 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 Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, 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;

"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 Contract as set out in the Award Letter;
"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 Contract 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;
"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;
"LED"	means Law Enforcement Directive (*Directive (EU) 2016/680*)
"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;
"Processing"	has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted accordingly;

"Processor Personnel"	means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract;
"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 including those outlined in Schedule 5 (Security Requirements and Plan);
"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 Contract;
"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 Contract;
"Services"	means the services to be supplied by the Contractor to the Authority under the Contract;
"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 Contract;
"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 Processor related to this Contract;
"Contractor Code of Conduct"	means the HM Government Contractor Code of Conduct dated September 2017;

"Term"	means the period from the start date of the Contract set out in the Award Letter 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 Contract;
"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 Charges 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 Contract;

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 Contract, 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 Contract.

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 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 Contract;

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.

3.4 Any Variation will not take effect unless recorded in a Change Control Notice in the form set out in Schedule 6 and approved in writing by the Authority.

4 Term

4.1 The Contract shall take effect on the date on 1st November 2019 shall expire on the 31st October 2020, 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 The Authority may extend the Contract for a period of up to 2 years with an annual review by giving not less than 10 Working Days' notice in writing to the Contractor prior to the Expiry Date. The terms and conditions of the Contract 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 the Award Letter appended hereto 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 Contract. 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 Contract, 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 Contract 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 Contract (including any sum which the Contractor is liable to pay to the Authority in respect of any breach of the Contract), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Contractor under the Contract 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, 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 Contract 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 Contract.

5.8.3 In this clause 5.8 'sub-contract' means a contract between two or more Contractors, 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 Contract.

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 Contract (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 Contract 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 Contract. Such equipment shall be returned promptly to the Authority on expiry or termination of the Contract.

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, 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 Contract, 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 and addresses (and any other relevant information) of all persons who may require admission to the Authority's premises in connection with the Contract;

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

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

7.2.5 ensure that it does not engage in any act or omission that would contravene Anti-Slavery and Human Trafficking Laws.

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, 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 and addresses 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 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 Premises.

7.7 The Authority may require the Contractor to ensure that any person employed in the provision of the Services has undertaken a Criminal Records Bureau check as per the Staff Vetting Procedures.

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 Contract or any part of the Contract. 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 Contract, 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 Cub-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:

(a) impose obligations on its Sub-Contractor on the same terms as those imposed on it pursuant to this Contract and shall procure that the Sub-Contractor complies with such terms; and

(b) provide a copy at no charge to the Authority, of any Sub-Contract, on receipt of a request for such by the Authority.

8.4 The Authority may assign, novate, or otherwise dispose of its rights and obligations under the Contract 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 Contract.

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 Contract 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 Contract for the sole purpose of enabling the Contractor to perform its obligations under the Contract.

9.2 All intellectual property rights in any materials created or developed by the Contractor pursuant to the Contract 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).

9.3 The Contractor hereby grants the Authority:

9.3.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Contract and any intellectual property rights arising as a result of the provision of the Services; and

9.3.2 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 Contract; and

b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Contract 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 the Authority reasonably requires in order to exercise its rights and take the benefit of the Contract including the Services provided.

9.4 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.

9.5 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 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 Contract, or as long a period as may be agreed between the Parties, full and accurate records of the Contract 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 Contract.

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 Contract.

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 on a need to know basis to enable performance of the Contractor's obligations under the Contract 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 Contract; and

11.2.6 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;

c) to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate 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 Contract is not Confidential Information and the Contractor hereby gives its consent for the Authority to publish this Contract 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 Contract 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 Contract 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 Contract or any part of the Contract 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 and 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 Contract 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 Contract, 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.

13 Protection of Personal 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, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

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

(c) ensure that:

(i) the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 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 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.

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

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

13.15 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.

13.16 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.

13.17 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 the Security Plan produced by the Contractor fully complies with Schedule 5 (Security Requirements and Plan).

13A.3 The Contractor shall comply, and shall procure compliance of its Staff, with Schedule 5 (Security Requirements and Plan).

13A.4 The Authority shall notify the Contractor of any changes or proposed changes to Schedule 5 (Security Requirements and Plan). Any changes shall be agreed in accordance with the procedure in clause 20.3.

13A.5 Until and/or unless a change to the Charges is agreed by the Authority, the Contractor shall continue to perform the Services in accordance with its existing obligations.

13A.6 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 Contract.

14.2 Subject always to clauses 14.3, 14.4 and 14.5:

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 Contract, 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 a sum equal to 125% of the Charges paid or payable to the Contractor whichever is higher;

14.2.2 except in the case of claims arising under clauses 9.4 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 Contract 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 under the indemnity in clauses 9.4 and 18.3 shall be unlimited.

14.5 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 Personal Data or any copy of such Authority Data or Personal Data shall in no event exceed one hundred thousand pounds (£100,000)

14.6 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 five million pounds (£5,000,000);

c) Professional indemnity with the minimum cover per claim of five million pounds (£5,000,000);

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 Contract.

15 Force Majeure

15.1 Neither Party shall have any liability under or be deemed to be in breach of the Contract for any delays or failures in performance of the Contract 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 Contract by written notice to the other Party.

15.2 Any failure by the Contractor in performing its obligations under the Contract which results from any failure or delay by an agent, sub-contractor or Contractor shall be regarded as due to Force Majeure only if that agent, sub-contractor or Contractor is itself impeded by Force Majeure from complying with an obligation to the Contractor.

16 Termination

16.1 The Authority may terminate the Contract at any time by notice in writing to the Contractor to take effect on any date falling at least 1 month (or, if the Contract 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 Contract 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 Contract which is not capable of remedy;

16.2.2 repeatedly breaches any of the terms and conditions of the Contract 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 Contract;

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; 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 Contract by written notice to the Authority if the Authority has not paid any undisputed amounts within 90 days of them falling due.

16.5 Termination or expiry of the Contract 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 Contract that either expressly or by implication has effect after termination.

16.6 Upon termination or expiry of the Contract, 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 Contract. 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 Contract.

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 Contract 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 Contract in accordance with all applicable equality Law and the Authority's equality and diversity policy as provided to the Contractor from time to time; 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 from time to time.

17.5 The Contractor shall comply with, and shall ensure that its Staff shall comply with, the provisions of:

17.5.1 the Official Secrets Acts 1911 to 1989; and

17.5.2 section 182 of the Finance Act 1989.

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 Contract or any other contract with the Crown (including the Authority) the Authority may:

18.4.1 terminate the Contract 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 Contract; 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 Contract 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 Contract, and that the Contract 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 Contract 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 Contract 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. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at clause 19.

20.5 The Contract 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 Contract on the basis of any representation that is not expressly incorporated into the Contract. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.

20.6 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Contract 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 Contract.

20.7 The Contract 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 Contract. 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 Contract, all remedies available to either Party for breach of the Contract (whether under the Contract, 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 Contract 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 Contract and rendered ineffective as far as possible without modifying the remaining provisions of the Contract, and shall not in any way affect any other circumstances of or the validity or enforcement of the Contract.

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 Contract. 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 Contract 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 Contract constitutes the entire contract between the Parties in respect of the matters dealt with therein. The Contract 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 Contract, no notice or other communication from one Party to the other shall have any validity under the Contract 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:

Address: 151 Buckingham Palace Road, London, SW1W 9SZ

For the attention of: [redacted]

Tel: [redacted]

Email: [redacted]

21.3.2 For the Contractor:

Address: 252B Gray's Inn Road, London, WC1X 8XG

For the attention of [redacted]

Tel: [redacted]

Email: [redacted]

21.4 Either Party may change its address for service by serving a notice in accordance with this clause.

21.5 Notices under clauses 15 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.

22 Governing Law and Jurisdiction

22.1 The validity, construction and performance of the Contract, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

23 TUPE – NOT APPLICABLE

IN WITNESS of which this Contract 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 .....[redacted]..

Position ....[redacted]..

SIGNED for and on behalf of **OFFICE FOR PUBLIC MANAGEMENT LTD TRADING AS TRAVERSE**[redacted]

Signature ..[redacted]..

Name .....[redacted]..

Position ....[redacted]..

SCHEDULE 1 – INVITATION TO TENDER AND SPECIFICATION

Public Research 1: Annual Awareness Survey

CQC is committed to ensuring people from a wide range of population groups feel that CQC is on their side, are enabled and encouraged to understand the standards of care they should expect and are empowered to encourage improvements to care.

CQC wants everyone who has cause to receive care or treatment from the services it regulates, to know about its role.

We want to measure levels of public awareness and understanding amongst a nationally representative sample (England only) in terms of age, Socio-Economic Group (SEG) and gender. This will be the fifth year of us running this survey, so we would want to compare progress against previous year's performance.

The sample must be sufficient to support further analysis (awareness and understanding) of the following groups:

- Carers
- people with a long-term condition
- 65+ year olds and
- people who have used a health care service in the past 6 months.

We would look for the tender to advise on the best approach to measuring public awareness, understanding and sentiment levels. We would anticipate this would be achieved via a quantitative survey approach.

Examples of the questions we would want to ask:

Q1 Are you aware that there is a regulator of health and adult social care services in England?

1. Yes

2. No

ASK IF YES AT Q1

Q2 What is the name of the regulator?

OPEN ENDED

ASK IF NO AT Q1

Q3 Have you heard of the Care Quality Commission (CQC)?

1. Yes

2. No

ASK IF YES AT Q3

Q4 What do you think the Care Quality Commission does?

OPEN ENDED

Q10 Do you have confidence that the Care Quality Commission can effectively monitor, inspect and regulate services?

Yes Don't know No

We anticipate around 30 questions in total with 3 or 4 open-ended and the rest closed questions. Many of the questions are fixed to give us continuity of analysis from previous years, but there is scope to introduce, or change to a couple of new questions.

We would expect most questions to offer pre-coded responses. For open ended questions, we would offer pre-coded responses for surveyors to select.

In terms of communicating the findings, we would look to the supplier to provide a presentation to CQC staff and produce a final report - format to be agreed with the supplier.

This research will include:

- Providing advice and expertise on the design and undertaking of the research. This will be used to measure current awareness of CQC in a transparent way. We expect the supplier to use the same methodology as previous years so that we are able to compare and contrast results and benchmark our surveys, Previous methodology requires using telephone surveys and computer assisted surveying techniques.
- Provide analytical support to process the results of the survey. CQC will also require a report that sets out the overall findings of the survey responses and a presentation of the results. This will enable CQC to assess the impact of its current engagement work on awareness.
- Outputs to provide CQC with information for targets to improve our activity and performance in raising awareness of the organisation. Outputs will also allow for CQC to assess the value for money and look for areas to increase efficiency in this work.
- We would like the supplier to provide recommendations on the back of their findings
- In terms of communicating the outputs, we would look to the supplier to provide a presentation to CQC staff and produce a final report - format to be agreed with the supplier.

Public Research 2: National Stakeholder Sentiment Survey

National stakeholder trust and confidence in CQC are key internal and external performance measures for evaluating the CQC's effectiveness, impact and value for money.

In order to monitor and report on progress in this area we need to benchmark stakeholder awareness and sentiment from a representative sample of national charities.

This will help us to look at areas to improve our performance and to ensure our work has maximum impact and value for money.

This research will include:

- Providing advice and expertise on the design and undertaking of the research. This will be used to measure current sentiment towards CQC in a transparent way. We anticipate that the supplier would advise on the best approach to measuring sentiment levels. We would anticipate that this would be achieved through a telephone survey.
- Providing analytical support to process the results of the survey. CQC will also require a report that sets out the overall findings of the survey responses and a presentation of the results. This will enable CQC to assess the impact of its current engagement work with these key stakeholders.
- Outputs to provide CQC with information for targets to improve our activity and performance with national charities. Outputs will also allow for CQC to assess the value for money and look for areas to increase efficiency in this work.
- We would like the supplier to provide recommendations on the back of their findings
- In terms of communicating the outputs, we would look to the supplier to provide a presentation to CQC staff and produce a final report - format to be agreed with the supplier.

We would anticipate that the research would involve around 25 interviews with priority stakeholders. We would expect the research to include free flowing interviews shaped by a set of questions agreed by CQC.

The research would focus on:

- The relationship the stakeholder has with CQC
- The stakeholders perception of CQC
- The organisational relationship the stakeholder has with CQC
- The stakeholders perception on their engagement with CQC

Public research; Additional research projects:

We require the supplier to complete additional research projects to respond the evolving needs of policy development. These are likely to be qualitative public research projects focusing on the changing landscape of health and social care and how CQC should respond to it. There will likely be a need for focus groups/ telephone interviews to be carried out. The supplier should provide expertise on the design and undertaking of the research. It would be expected that the supplier provide analytical support to report on the qualitative findings and present these in a written report and presentation.

Previous examples include research projects such as:

- New models of care- what "good" looks like
    - We wanted to understand how best we could communicate to patient representative organisations and the public around new models of care and what they could expect from these. We asked the supplier to determine "I" statements for eg "new models of care are good when I am assured that there is one person taking ownership of the situation…". We also sought to find what people wanted to be communicated to them.
- Whistleblowing research
    - This was undertaken with providers and professionals as part of public research as enabling people to report experiences on our website falls into public engagement's remit.
- Public research findings around digital primary care, including what "good" looks like
    - We wanted to talk to people who had experience of using digital primary care services and find out concerns from those who never had. We also wanted to know what good looks like to the public and we used "I" statements to help determine this in line with our Key Lines Of Enquiry (KLOEs)

For all research projects, we would expect the participants to be fully aware of what they are signed up for, so there would be no use of covert research methods

This research will include:

- Providing advice and expertise on the design and undertaking of the research. This will be used to measure current sentiment towards CQC in a transparent way. We anticipate that the supplier would advise on the best approach to measuring sentiment levels. We would anticipate that this would be achieved through a telephone survey.
- Providing analytical support to process the results of the survey. CQC will also require a report that sets out the overall findings of the survey responses and a presentation of the results. This will enable CQC to assess the impact of its current engagement work with these key stakeholders.
- Outputs to provide CQC with information for targets to improve our activity and performance with national charities. Outputs will also allow for CQC to assess the value for money and look for areas to increase efficiency in this work.
- We would like the supplier to provide recommendations on the back of their findings
- In terms of communicating the outputs, we would look to the supplier to provide a presentation to CQC staff and produce a final report - format to be agreed with the supplier.

Key Performance Indicators:

Indicator	Measured by	Reference Point or Target	Review Date
Schedule adherence	The schedule must be adhered to as outlined in the project plan. The supplier is required to meet the deadlines agreed upon	Timeline as agreed with by CQC 100% critical KPI	Bi weekly review dates
Supplier outputs	The supplier is required to deliver survey outputs as agreed upon in the project plan. For our NSSS and AAS, these should reflect previous survey methods and questions so as to enable benchmarking. We require the raw data as well as analysed reports and summary of findings. For the other research these should be delivered in agreement with CQC. Summary: report to be delivered within the time frame agreed in the project plan, likely to be within 1 week of completion of fieldwork.	Project plan as agreed with CQC. 100% critical KPI	Bi weekly review dates
Attendance at meetings	The supplier is required to attend all planned Operational Delivery (as outlined in Contractor Responsibilities), Performance Review and End of project	Review meetings attended as outlined in project plan 100% critical KPI	Bi weekly review dates

	review meetings, unless otherwise agreed with the Authority. A face to face meeting to present the final report at CQC offices is required. We would require a dedicated project manager to act as key point of contact		
Supplier availability	The supplier should reply to queries within 24, hours with queries resolved within 72hours, maintaining adherence to agreed schedule	Email dates when query opened or from meeting date where query was raised 95% non-critical KPI	Bi weekly review dates
Service level agreements	Meeting agreed service levels (according to timeline in project plan) • AAS- the supplier will have spoken to 1000 people, • NSSS- supplier will have spoken to 25 people Using methods as agreed in the project plan. The supplier is required to ensure that there are sufficient personnel and other resources to deliver the work packages on time and to the quality standards required.	Project plan 100% critical KPI	Bi weekly review dates

	We would require a dedicated project manager to act as key point of contact. The supplier will be contactable to the Authority between the hours of 9am to 5pm Monday to Friday For other research projects, as agreed in the project plan		
Security Requirements	Services will be delivered in accordance with information security, data protection, GDPR, any confidentiality requirements including those agreed with the Confidential Advisory Group (CAG). This is the supplier's responsibility as they are providing us with anonymised data. The supplier will advise CQC where any such breach occurs. **This needs to be done within 24hours of the breach being identified**	100% Critical KPI	Over duration of project
Demonstrate flexibility upon feedback	Feedback incorporated, unless justified and agreed with CQC not to incorporate it	Feedback visible in further work done 97% critical KPI (the 3% accounts for the estimated feedback that may not be included, as agreed with CQC)	Bi weekly review dates

Evaluation and learning	Evaluation and learning will be completed at the end of each delivered package, and any identified improvements flagged along with an action plan for development. This should be done within 2 weeks of the main presentation of findings.	Over the duration of the project 95% Non-critical KPI	Bi weekly review dates
Quality of Expertise	The supplier is to ensure that individuals providing support to the public research programme are those stated in the response or an equivalently qualified individual where the stated personnel have left.	Evaluated at start, of project and again if individuals change. 100% critical KPI	Bi weekly review dates

Milestones:

We currently cannot specify exact dates, rather general timelines. We expect an individual project to take place over 3 months, usually between q1 and q2. The timeline below can be applied to each project over the duration of the contract.

Description	Target Date	Action to Achieve Milestone	Review Date
Kick off call	Day 0	• Attend the kick off meeting	Date of kick off meeting
Draft survey submitted	Week 2	• CQC have received a copy of the draft survey in-line with agreements made on kick-off call	Agreed date for receiving survey.
Comments from CQC	Week 3	• CQC send comments back to the supplier	Within 1 week of having received the draft survey. Reviewed on the agreed date.
Survey signed off	Week 4	• CQC send confirmation to supplier that they are satisfied with the survey	Signed off by agreed date
Research commences	Week 5-8	• Supplier commences research and starts research. E-mail to CQC to confirm.	Week after research commences
Interim feedback	Week 7	• CQC receives interim findings from the supplier.	By agreed date for interim feedback
End of project feedback	Week 8.5	• CQC receives verbal summary of overall findings from supplier	Within 1 week of concluding research phase
Draft report	Week 9-10	• CQC receives draft report from the supplier	By agreed date, within 1.5 weeks of verbal feedback.

Comments from CQQC	Week 11	• CQC send comments back to supplier on findings	Within 1 week of receiving draft report
Final Report	Week 12	• Final report submitted to CQC with all amends incorporated.	Within 1 week of receiving CQC comments
Presentation of report	Within 3 weeks of final report	• Presentation version of report made and date agreed or presentation	Delivered within 3 of final report completion

SCHEDULE 2 – CHARGES

Cost Envelope

Total contract value including VAT will be up to a maximum of **£85,000** per annum

Day Rate Card

Role Level	Day Rate (Ex. VAT)	Day rate (Inc. VAT)
[redacted]		

[redacted]

Statement of Works

The Statement of Works document below will be used for each individual piece of work to capture requirements and costs.

Once requirement have been determined, CQC will provide Office for Public Management Ltd trading as Traverse with the document below.

Office for Public Management Ltd trading as Traverse are required to complete the Statement of Works within a determined timeframe prior to any work commencing

Statement of Works

1. REQUIREMENTS
(1.1) Services required including any key personnel:
(1.2) Commencement Date:
(1.3) End Date:
(1.4) Key Personnel of the Contractor
(1.5) Quality/Technical/Performance Standards
(1.6) Location(s) at which Services are to be provided:

2. PRICE AND PAYMENTS
(2.1) The Price excluding VAT, payment profile and method of BACS)) [ ]] Guidance: Insert details of the Price, payment profile and method of payment.
(2.2) Invoicing and Payment The Contractor shall issue invoices [monthly]/[quarterly] in arrears. Guidance: if known, specify any additional supporting information which the Contractor should provide with the invoice.

3. COMMERCIALLY SENSITIVE AND CONFIDENTIAL INFORMATION
The following information shall be deemed Commercially Sensitive Information or Confidential Information: [ ] [Guidance: Include details of any Commercially Sensitive Information identified by the Contractor and the duration it should be confidential for. This will assist the Authority in respect of compliance with Freedom of Information Act and the section 45 Code published by the Department of Constitutional Affairs.]

4.NOTICES
Notices shall be sent to the addresses set out below for the purpose of service of notices under the Call-Off Contract: **For the Authority:** Contact Name: Address: Email: **For the Contractor:** Contact Name: Address: Email:

BY SIGNING AND RETURNING THIS ORDER FORM THE CONTRACTOR AGREES to enter a legally binding contract with the Authority to provide to the Customer the Services specified in the Order Form, incorporating the Care Quality Commission Terms set out in the agreement entered into by the Contractor and the Authority on **1st November 2019**.

For and on behalf of the Contractor:

Signed _____

Name _____

Position _____

Date _____

For and on behalf of the Authority:

Signed _____

Name _____

Position _____

Date _____

SCHEDULE 3 – TENDER RESPONSE

Overview

As outlined in the Statement of Requirements, CQC want to commission independent, transparent and robust research to support delivery of key priorities within your current Strategy. The approach to the research will ensure your audiences inform the shape of CQC improvements, and evidence produced will provide you with information about current awareness, understanding and sentiment toward CQC among the public and charity sector stakeholders. Our recommendations will focus on ways to increase efficiency in your work in these areas.

Traverse has extensive experience of working with CQC, including 2018 public research into digital primary care, 2017-18 consultation on new models of care, and 2016 annual awareness survey (as OPM Group). We are familiar with CQC's organisational needs and priorities, and the broader health and social care environment. Other current clients in the regulatory and health workforce sectors include the Nursing and Midwifery Council (NMC) and Health Education England (HEE).

We see ourselves as a partner, working closely and collaboratively with our clients to support the design of research that effectively helps them to achieve their strategic goals. We recently conducted an online survey and telephone interviews for the Association of the British Pharmaceutical Industry to explore stakeholder attitudes and views towards their Code of Practice, and are currently helping the NMC to engage with stakeholders, including the public, to inform their Future Strategy development.

We recognise the importance of fidelity to the previous years' methods for the annual awareness survey (ASS). This is reflected in the methods we propose to use (CATI survey). By working with our trusted fieldwork partner, Qa Research, we are confident in achieving the required sample to generate meaningful and comparable data. We will also aim for a high level of fidelity in the national stakeholder sentiment survey, while allowing for new and current issues to be explored and captured.

We bring our strong track record of engaging charity sector leaders in the National Stakeholder Sentiment Survey (NSSS) and will work with you to ensure that the final sample, and design of questions generate relevant evidence.

Our proposal for the additional public research is intended to give an example of what is possible within the available budget. We look forward to working with you to determine the scope and design of this work.

As part of our commitment to provide applied recommendations as an output from the research we offer a facilitated "routes to action" workshop.

Leadership

[redacted] will be responsible for overseeing the research, ensuring consistency and quality. She will manage three dedicated project managers for each strand of work. All have particular methodological strengths in the strands for which they are responsible.

[redacted]

[redacted]

[redacted]

Method Statement

1. **Annual awareness survey**

We understand that comparability with previous years' survey data is vital and will replicate the methods used, i.e. computer assisted telephone survey of 1000 participants. This will be conducted by our trusted partner Qa research. Up to 30 questions, 3-4 of which to be open, will be provided by CQC, and interviews will last up to 15 minutes.

A contact database will be purchased from DBS Data, and a sample matrix devised to ensure a nationally representative sample by age, gender, region & social economic grade (SEG). Screener questions will be included at the beginning of the survey to monitor these. Sub-samples (carers, long term conditions, 65+ year olds and recent use of health care service) will be included in the sample (minimum 100 for each group).

We will work with you to refine any questions as necessary to best meet your requirements for measuring awareness, understanding and sentiment levels.

1. **National stakeholder sentiment survey**

We will generate a target sample of interviewees in national charities based on a contact list provided by CQC, and undertake 25 free-flowing telephone interviews in order to understand their relationships with and perceptions of CQC, and reasons behind these.

We will segment potential interviewees by type of organisation (e.g. size and disease/condition focus) and type of interviewee (e.g. communications, policy, engagement, senior leadership) in order to achieve a broadly representative sample. We suggest contacting 50 potential interviewees in the first instance in order to achieve the target of 25; we recommend an email introduction from CQC with subsequent follow-up by Traverse, by email and telephone.

Interviews will last 30mins-1 hour at a time convenient to participants.

We will assure participants of anonymity in our reporting, so they feel comfortable sharing their views.

We anticipate revisiting the questions asked in previous surveys to enable benchmarking where possible, and developing this set of questions with you in order to capture data around specific current priorities.

2. **Additional public research**

You require additional, qualitative research to support evolving policy development in a fast-changing environment. We will work closely with you not only to design and undertake the research but also to support thinking around the scope and focus of the research project, or projects, to ensure that they meet your wider engagement needs.

Our proposal provides an indicative example of what is possible. We have provided costs for four focus groups of up to 8 participants, in different geographical locations, sampled to include a range of characteristics, to be recruited using an agency, hosted in external venues and incentivised with £40 thank you payment. Within this overall budget there is significant flexibility according to what research need(s) arise and which audience(s) these involve. For example:

- we could hold two larger workshops, or 25 telephone interviews, instead of 4 focus groups, or a mix of activities; these options and numbers could be further varied depending on the factors below
- depending on the target audience we could recruit via community/support organisations, thereby reducing recruitment and venue costs significantly
- we could vary the range of locations of the fieldwork.

The additional research would be led by a Traverse consultant who managed the research into what good looks like in online primary care (one of the examples in your specification), in 2018 (as with the other projects, supported and overseen by [redacted]

Analysis and reporting

AAS: quantitative data will be run through advanced analysis software Askia and include cross-tabulations to identify statistically significant differences by sub-groups. Weighting will be applied to correct imbalances in sample profile. Comparison with the previous year's data will be undertaken, and with data from all previous years (assuming that at least some questions have been consistent) to enable trend analysis.

Qualitative research (NSSS and additional): we will analyse detailed interview notes (supported by audio recordings) using an agreed analysis framework and use a qualitative analysis software package to code data against themes, initially likely to be the interview questions and sample segmentation based, then further refined according to the content of the data.

We will produce separate reports for each project, in a format that is most helpful to CQC. Reports will be written in plain English and include a short summary of key findings. The recommendations must identify areas to improve CQC's performance and maximise impact and value for money; they must also be practical to implement, and we will work closely with you to develop these. We are keen to discuss a facilitated 'routes to action' workshop to help share and embed the recommendations among key colleagues and stakeholders.

Timeline

The timeline is a draft based on our experience and that of Qa Research of how these projects may pan out in practice; we would refine this during project set up, drawing on the example in your specification.

Oct-Dec 2019	w/c 07-Oct	14-Oct	21-Oct	28-Oct	04-Nov	11-Nov	18-Nov	25-Nov	02-Dec	09-Dec	16-Dec	Xmas period	06-Jan
Annual Awareness Survey													
Inception meeting													
Survey design, sign off and programming													
Survey in field													
Survey closes													
Analysis and reporting													
Presentation (two options)													
National Stakeholder Sentiment Survey													
Inception meeting													
Stakeholder scoping and recruitment													
Interview topic guide design and sign off													
Stakeholder interviewing													
Analysis and reporting													
Presentation (two options)													

Jan-Mar 2020	06-Jan	13-Jan	20-Jan	27-Jan	03-Feb	10-Feb	17-Feb	24-Feb	03-Mar	10-Mar	17-Mar	24-Mar	within 3 weeks
Additional public research													
Inception meeting													
Sampling and recruitment													
Design													
Fieldwork													
Analysis and reporting													
Presentation													

Quality assurance and risk management

Our quality and risk management approach manages potential risks to the project and ensures high quality processes and outputs. It is certified to ISO 9001 and 27001 and sensitive data is handled in compliance with the Data Protection Act 2018 and UK implementation of EU GDPR.

We have a clear internal governance structure, with senior team members taking responsibility for quality control. Our key internal processes to ensure high quality delivery include internal briefings, regular supervision and analysis and reporting protocols.

Our collaborative approach with clients, partners, and participants is underpinned by rigorous principles of transparency, integrity and clarity and ensures that project management remains flexible and responsive to change. At the outset, the Project Manager will prepare a timeline outlining key dates and milestones, which is reviewed regularly; should any risks be

identified we will propose assigning additional resources or changing working practices, for CQC's approval.

We have drafted an initial risk register to be developed with you:

Risk	Severity	Mitigation
Generic		
Key staff are absent	Low likelihood, low impact	Internal team includes individuals able to deliver any of the required roles. Any member of the team who is out of the office for more than 48 hours has a protocol for handing over their work to others.
Quality of deliverables does not meet CQC expectations	Low likelihood, high impact	We will work with you from the outset to agree how the report will look and feel, and discuss emerging findings with you so there are no surprises.
Annual Awareness Survey		
Difficulties achieving interviews within the time period	Low likelihood, high impact	We are working with Qa research who have a dedicated telephone team set up to conduct the survey. They conduct calls during the day, evening and at the weekend and offer a Freephone telephone number to enable individuals to call at a time convenient to them, if they prefer.
Issues with the comparability of data	Low likelihood, high impact	We propose mirroring the approach of previous annual surveys to retain ability to compare
Stakeholder sentiment survey		
Lack of availability within the timeframe	Medium likelihood, high impact	Accelerated set-up phase to ensure we are able to send out invites almost immediately. Option to consider alternates within an organisation, or approach a wider range of organisations to hit the quotas.
Interviews impact negatively on perceptions of CQC	Low likelihood, medium impact	When conducting interviews we will be representing you in the eyes of stakeholders. We will field experienced researchers to conduct the interviews to ensure that a professional and positive impression is made.

Resource Plan

Resource Plan

Annual Awareness Survey
Set up meeting
Survey design
Telephone interviews (Qa Research)
Analysis
Reporting
Presentation
Project Management

[redacted]

National Stakeholder Sentiment Survey
Set up meeting
Interview topic guide design
Sampling and recruitment
25 interviews (incl 2 days set-up)
Analysis
Reporting
Presentation of findings
Project management

[redacted]

Additional public research
Set up meeting
Design - overall project
Materials design
Sampling
Recruitment
Venue booking and liaison
Facilitation
Analysis
Reporting
Presentation of findings
Project management

[redacted]

Exit Strategy and Skills Transfer

It is imperative that the supplier of this work provides CQC all the requisite knowledge, including research tools, data and project learning, for the survey(s) to be repeated in the future with a high degree of fidelity. You need this in order to analyse trends and changes in stakeholder awareness and sentiment over time.

On completion of the work we would transfer to you:

- The raw datasets and weighted data tables
- Final research materials (survey questions and interview guides)
- A detailed, transparent and replicable methodology, as part of each final report. This will include details of sample quotas and matrix, source of contact list used to select interviewees, details of the analysis process used and source of statistical information used to apply weighting.
- A set of reflections on the research process including learning from any challenges and solutions/mitigations
- We are also keen to work with you to ensure that the AAS and NSSS are routes through which you can annually gather data to allow you to assess value for money of your awareness raising activities, plus other useful metrics.

We would be happy to have a project de-brief meeting with you, pro-bono (separate to the routes to action presentation of findings), to ensure that knowledge and information are transferred to the relevant colleagues within CQC, and that they are comfortable in taking ownership of this knowledge in relation to future ASS and NSSS procurement.

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The contact details of the Controller's Data Protection Officer are: Nimali de Silva, Care Quality Commission, 3rd Floor, Buckingham Palace Road, London SW1W 9SZ.

2. The contact details of the Processor's Data Protection Officer are: [redacted]

3. The Processor shall comply with any further written instructions with respect to processing by the Controller.

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

National Stakeholder Sentiment Survey (NSSS)

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with Clause 13.1.
Subject matter of the processing	The NSSS is a yearly survey to understand how stakeholders feel about CQC's work/how we work with them.
Duration of the processing	For the duration of the contract. This is likely to be July-September every year, however this is subject to change by CQC depending on circumstances. In 2019 we would expect the results to be published by the end of 2019.
Nature and purposes of the processing	CQC will provide a list of names and contact details for representatives of stakeholder organisations to the contractor. The contractor will create a sample to contact from this list, to ensure appropriate representation

	based upon the organisation's representation of British population and job levels of staff The contractor will store the personal data securely and use it to contact people by phone or email and ask them to take part in the survey. They will monitor to see whether they have responded and follow up with reminder emails or phone calls Information gathered in responses will be used to create an anonymized data set (i.e. the information will not be identifiable or linked to a person or organization) and this will then be analysed and used by the data processor to create a report. The contractor will exercise reasonable care to ensure that individual data subjects are not identifiable within the report. We will publish this report on the CQC website and promote via our online channels, such as social media, crowd sourcing platform and news bulletins (emails).
Type of personal data	CQC will share names, job titles, organisations and contact details (i.e. phone number and email) with the data processor. The data processor will gather the views of these people about CQC.
Categories of Data Subject	Representatives of stakeholder organisations identified by CQC.
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	CQC will instruct the contractor on retention and disposal of personal data, in writing, once the contract is in place. The contractor will retain, and return/dispose of/destroy personal data strictly in accordance with any written instruction from CQC.

Annual Awareness Survey (AAS)

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with Clause 13.1.
Subject matter of the processing	The AAS is a yearly survey to understand what the awareness of a representative sample of the population is about CQC and ascertain trends in awareness and of different population groups The contractor, on behalf of CQC, will obtain demographic data and contact information in order to conduct research with a sample of the population of England.
Duration of the processing	For the duration of the contract. This is likely to be July-September every year, however this is subject to change by CQC depending on circumstances. In 2019 we would expect the results to be published by the end of 2019.
Nature and purposes of the processing	The data processor will create a sample to contact based on a representative sample of the English population. The contractor may use a 3rd party recruitment agency that fulfills GDPR requirements and works in line with the contract that is held with CQC, but CQC must be made aware of, and approve, the use of any third party processors being used. The contractor will be responsible for the actions of any sub-contractor they engage. The contractors process for obtaining demographic data, contact info and contacting people will be agreed between CQC and the contractor in writing prior to commencement The demographic data will be used to ensure we have a representative sample of the English

	population that will be surveyed. The contact data will be used to contact the selected people. Information gathered in responses will be used to create an anonymized data set (i.e. the information will not be identifiable or linked to a person or organization) and this will then be analysed and used by the data processor to create a report. The contractor will identify any protected characteristics groups that they have engaged with through the demographic information they have collected but this will be anonymized for CQC. The contractor will exercise reasonable care to ensure that individual data subjects are not identifiable within the report. We will publish this report on the CQC website and promote via our online channels, such as social media, crowd sourcing platform and news bulletins (emails).
Type of personal data	The data processor will collect names, age, questions around protected characteristics and contact details (ie phone number and email), though names will only be used for the purpose of addressing the person in the phone call.
Categories of Data Subject	Members of the public
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	CQC will instruct the contractor on retention and disposal of personal data, in writing, once the contract is in place. The contractor will retain, and return/dispose of/destroy personal data strictly in accordance with any written instruction from CQC.

SCHEDULE 5 – SECURITY REQUIREMENTS 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 5.

"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.

"Protectively Marked" shall have the meaning as set out in HMG 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 HMG 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 HMG 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 19 (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 Variation and shall not be implemented until Approved.

5. AUDIT, TESTING AND PROTECTIVE MONITORING

5.1 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.

5.2 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.

5.3 Where any Security Test carried out pursuant to paragraphs 5.1 or 5.2 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 HMG 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 variation procedure set out in the Contract.

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

In accordance with clause 16 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. SECURITY CLASSIFICATION OF INFORMATION

1.1 If the provision of the Services requires the Contractor to Process Authority Data which is classified as OFFICIAL, OFFICIAL-SENSITIVE or Personal Data, the Contractor shall implement such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable legislative and regulatory obligations.

2. END USER DEVICES

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

2.2 The Contractor shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

2A. TESTING

The Contractor shall at their own cost and expense, procure a CHECK or CREST Certified Contractor to perform an ITHC or Penetration Test prior to any live Authority data being transferred into their systems. The ITHC scope must be agreed with the Authority to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority data.

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 not, and shall procure that none of its Sub-contractors, process Authority Data outside the EEA without the prior written consent of the Authority and the Contractor shall not change where it or any of its Sub-contractors process Authority Data without the Authority's prior written consent which may be subject to conditions.

3.3 The Contractor must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority data has been stored and processed on.

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 when transmitted.

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 Contractors should design the service in accordance with:

- NCSC " Security Design Principles for Digital Services "
- NCSC " Bulk Data Principles "
- NSCS " Cloud Security Principles "

6. PERSONNEL SECURITY

6.1 All Contractor Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Contractor maybe required implementing additional security vetting for some roles.

7. IDENTITY, AUTHENTICATION AND ACCESS CONTROL

7.1 The Contractor must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Contractor must retain records of access to the physical sites and to the service.

8. AUDIT AND PROTECTIVE MONITORING

8.1 The Contractor shall collect audit records which relate to security events in delivery of the service 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 regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any

unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data. The retention periods for audit records and event logs must be agreed with the Authority and documented.

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 8.3 for a period of at least 6 months.

9. VULNERABILITIES AND CORRECTIVE ACTION

9.1 Contractors shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

9.2 Contractor must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Contractor COTS Software and Third Party COTS Software are always in mainstream support.

10. RISK ASSESSMENT

10.1 The Contractor should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

ANNEX 2: CONTRACTOR'S SECURITY MANAGEMENT PLAN

Traverse Security Management Plan

Traverse has a comprehensive Information Security Management Plan which has been accredited to ISO 27001. Please find attached the following key policies and procedures:

- Traverse Quality and Information Security Policy Statement (we run a combined ISO 9001 and ISO 27001 system)
- Sensitive Data Management
- Document Classification
- Data Protection Policy
- Information Security Incident Reporting Procedure.

Traverse's approach to quality and information security is set in the context of our values as an independent, employee-owned, social results business.

At Traverse, we are committed to achieving standards of excellence in the provision of all our services. We aim to become the provider of choice for relevant services in our sectors by consistently meeting our clients' requirements and providing services of the highest quality.

Specifically, our ambition is to be:

- The leading provider of consultation services for complex and controversial public issues.
- A leading provider of social research and engagement services in the UK.
- The market leader in understanding, measuring and evaluating social impact.
- An exemplar employee owned business that models how to get the best out of our people.

We are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation, in order to meet our business objectives, clients' and relevant parties' requirements, legal and contractual obligations and maintain its competitiveness and commercial image.

The Directors accept full responsibility for ensuring that we achieve high quality in everything we do. We are responsible for ensuring that every client assignment is carried out by suitably qualified, trained and experienced staff working to proven quality procedures and with appropriate management and support.

Terry Parker

Chief Executive — 8 June 2019

Quality Policy

One of Traverse's Directors, Terry Parker, is nominated by the Board to act as a quality champion. The quality champion works closely with our quality manager, Marcus Clissold-Lesser who is responsible for supporting the implementation of Traverse's quality policy and procedures on a day-to-day basis.

All Traverse members are expected to up-hold the quality policy and follow quality procedures. Partners, associates, and suppliers are also expected to comply with these requirements.

At Traverse we pride ourselves on offering innovative services that meet new or emerging, as well as established, client needs. For every project, and especially when conducting highly innovative work, we work closely with our clients to identify appropriate indicators of quality and to ensure these are met consistently.

To ensure that we provide services of a consistently high quality, Traverse has a comprehensive quality management system in place. This has been designed to meet the requirements of the International Standard for Quality and is subject to regular internal and external assessment and review.

Traverse's quality management system has been approved and certified as complying with BS EN ISO 9001:2015.

Traverse's commitments to quality are set out in our Quality Manual. We also have detailed quality procedures covering every aspect of our work.

The most important components of Traverse's quality system, which are set out in more detail in our quality procedures, are as follows:

- Ensuring that high quality and suitably qualified staff are recruited into the organisation, by having rigorous and fair recruitment procedures in place.
- Ensuring all staff are supported in carrying out their role and exercising their responsibilities to a high standard through robust line management arrangements, regular appraisal and appropriate training and development opportunities.
- Working closely with our clients to establish appropriate indicators of quality, monitoring these on a regular basis, and seeking regular feedback, including at the end of each project.

Employing robust project management arrangements, with clear roles and responsibilities and appropriate procedures for client liaison and managing risk.

- Having clear procedures in place to identify and quickly resolve concerns and complaints.
- Ensuring that our partnering and use of associates are well and consistently managed to enhance our work for clients, through consistent monitoring and quality assurance
- Ensuring that we comply with all relevant legal requirements and meet industry standards, including in relation to health and safety and the storage of sensitive information.
- Ensuring that we continue to meet our clients' expectations by setting quality objectives, monitoring our progress against these, and regularly reviewing and improving our approach to quality through internal and external assessment.

Information and Security Policy

Traverse's information security management system (ISMS) has been approved and certified as complying with BS EN ISO 27001:2013 and will continue to be aligned with its business context, objectives and subject to continual improvement. The ISMS is intended to be an enabling mechanism for safe information sharing for operations and for reducing information-related risks to acceptable levels.

The Board has designated a team formed of experienced managers and key information owners to [redacted]

- Review the information security performance and the continuing suitability, adequacy and effectiveness of the ISMS;
- Support the ISMS framework and periodically review the security policy;
- Identify threats and vulnerabilities to assets and the likelihood and impact of these on maintaining the confidentiality, integrity and availability of its information assets;
- Establish measures of effectiveness of security controls;
- Collate, analyse and identify corrective, preventive and improvement measures;
- Ensure that members, partners and associates meet the security requirements through education and awareness training.

Traverse's Chief Executive and Board are fully committed to this policy and to ensuring that it is implemented in full, as well as supporting subsidiaries to achieve recognised information security standards. All Traverse members are expected to uphold this information security policy and follow security procedures.

[redacted]

Traverse Sensitive Data Management

Objective

To define the appropriate levels of protection to secure information being held by Traverse on behalf of its clients, interested parties or sensitive corporate information from accidental or malicious damage, modification or disclosure.

Scope

This policy applies to all users accessing Traverse information or information systems. It applies to:

- Information that is being held for clients, whether Traverse gathered that data or if the data was passed to Traverse, as a data processor.
- Information collected by Traverse for its own purposes such as personal staff data.

Related documents

- Document Classification
- Access Control
- Mobile ICT and teleworking
- Operations Manual
- IS Consideration Form

Responsibilities

The responsibilities for this policy lie with the Group Chief Executive, Board, HoDs and Risk Owners and all Traverse staff for ensuring that sensitive information is protected at all times especially remote from premises.

Project Manager to consider information security on a project basis taking into account the use of identifiable data and in particular when information is transferred across the internet, held on portable devices or any type of removable media. To select existing controls to protect the confidentiality, integrity, and availability project's information and to report any breaches.

System Support Manager is responsible for finding and suggesting advice and/or mechanisms by which the corporation can satisfy its obligations. All in house or outsourced solutions are used in compliance with all relevant agreements, legislation and regulations.

System Support Manager is responsible for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys

All cryptographic keys are protected against modification and loss and against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys is physically protected.

Requirements

Traverse is registered under the Data Protection Act as a data controller in its own right and also often acts as a Data Processor on behalf of its clients. Traverse recognises the importance of this duty of care and following its Risk Assessment procedure has identified that controls must be used to ensure that data is securely transmitted as well as stored on site.

- Information security consideration is used by project managers to determine the need for the protection of information and based on Traverse's Classification policy, Access control policy and whether sensitive or critical data are digitally transferred or used in transit.
- All critical or sensitive data transferred outside Traverse should be sent through DataSend or password protected with 7zip.
- All critical or sensitive data that is transported should be protected by a password. USB stick for example would need to be encrypted with password access; portable electronic devices such as laptops, mobile phones should be protected by passwords.
- An access right to password information is restricted on to a "need to know" basis.
- All security incidents, or potential unauthorised access to Traverse information and information systems, should be reported immediately to the IS Manager and/or Project Manager in accordance with Incident reporting.
- Users must be made aware of their responsibilities in the prevention of unauthorised access to Traverse information and information systems, including, but not limited to, the need to protect all sensitive or critical data which is to be transported or transmitted.

What is Sensitive Data?

Traverse considers as sensitive data:

- Any data which would fall under the remit of the Data Protection Act or the General Data Protection Regulations
- Any commercially sensitive data
- Any pre-public release collation data
- Any data entrusted to us in confidence by a client

Measures

Traverse has measures to securely store and transmit sensitive data.

Data Classification Policy

Objective

The purpose of classifying documents is to:

- protect them from unauthorised access (confidentiality)
- protect the integrity of the document by outlining editorial rules
- ensure availability of the document when required.

Scope

This policy covers all Traverse documentation.

Responsibilities

The responsibilities for this policy lie with the Group Chief Executive, Board, HoDs, Risk Owners, staff, contractors and third party users of Traverse information systems and services.

Definitions

Open

Documents classified as OPEN are not commercially sensitive and would not damage or compromise Traverse or our clients if they were publicly available.

For example, finalised marketing materials; finalised publications, most hand-outs, anything in the public domain.

The owner / author should mark the document OPEN but may wish to impose editing restrictions on these documents.

Restricted

Such documents are sensitive and may cause reputational, legal or other damage to Traverse and / or interested parties. **These documents can be sent to specific and relevant external parties.**

For example, policies and guidelines; draft marketing materials and publications; draft proposals; fee earner rates; draft reports; client specific documents; finalised proposals.

The owner / author is responsible for version control, imposing access and editing restrictions, and appropriate archiving or destruction as stated in Archiving and destruction policy.

They may mark the document RESTRICTED if they believe it will be helpful, although this is not necessary as RESTRICTED status is assumed for all documents if not otherwise marked. Older documents market Restricted Internal or Restricted External should both be considered Restricted under the new convention.

The user is responsible for appropriate transmission and proper storage of the document in accordance with Sensitive data management policy.

Confidential

Such documents are highly sensitive, and would cause significant reputational, legal or other damage to Traverse and / or interested parties.

For example, business plan; board papers; HR records and papers; ESOT papers; anything containing personally identifiable data; 360 reports; non-anonymised surveys; contracts; coaching notes; psychometric reports; payroll information; risk assessment; security incidents; budget information.

The owner / author is responsible for marking these as 'CONFIDENTIAL', version control, imposing access and editing restrictions, and appropriate archiving or destruction of the document (as per Archiving and destruction policy). They must also give permission for the document to be taken off site (in hard copy or electronically form).

The user is responsible for appropriate transmission and proper storage of the document in accordance with Sensitive data management policy.

Implementation

- Note Most documents are likely to be RESTRICTED. Therefore, any document with no marking should be treated as RESTRICTED.
- Any member of staff who identifies a potentially mis-labelled document should notify the project director for the label to be reviewed.
- Where a client requires specific naming conventions these will supersede Traverse's internal system. To minimise the risk of a document will be included in the project folder which maps the client classifications to Traverse's to ensure there is no ambiuity.

Handling guidelines

Please refer to the table below for full handling restrictions on classified documents.

Category	Open	Restricted	Confidential
Data processing and storage *GDPR – General Data Protection Regulation*	Data must be used in accordance with the GDPR	Data must be kept safe from unauthorised access, accidental loss or destruction	Data must be kept safe from unauthorised access, accidental loss or destruction
Marking on document	Open or Unclassified	None – this is assumed classification level	Confidential
Can document be taken off site?	Yes	Yes, for use by relevant people only	Authorisation from owner/author needed.
Digital transfer restrictions	None	Email to internal account holders or send external using DataSend or 128-BIT AES encryption or passworded 7Zip	Use DataSend or 128-BIT AES encryption or passworded 7Zip
Fax restrictions	None	Do not fax (unless specified in client contracts)	Do not fax
Post / courier restrictions	None	Use tracked courier where appropriate - refer to client requirements	Tracked courier with signed for delivery
Reproduction restrictions (printing, copying)	None	As appropriate - refer to client requirements where necessary	Do not reproduce unless you have permission from the owner/author
Permissions: access	Anyone can access	Only relevant people can access (e.g. project team)	Only relevant people can access (e.g. Client, Project team, Line managers, Board, ESOT)
Permissions: editing	Consider limits to editing rights	Owner/author-specified limits to editing rights	Owner/author-secified limits to editing rights
Internal storage inc removable media	Unlocked storage	Locked or encrypted storage	Locked or encrypted storage
Paper data archiving and destruction	In accordance with Archiving and destruction policy	In accordance with Archiving and destruction policy Shred	In accordance with Archiving and destruction policy Confidential shred where required (use red recycling bags)
Digital data archiving and destruction	Normal deletion	Secure destruction by the ICT team	Secure destruction by the ICT team

Data Protection Policy

Traverse regards the lawful and correct treatment of personal information as very important and therefore ensures that personal information is treated as such. Traverse management is committed to protecting individual information and endorse the principles of the Data Protection Act 1998, and the General Data Protection Regulation (in force 25 May 2018) which form part of its corporate practice, governance regime and its fundamental objectives to maintain confidence with clients, third parties and employees.

Personal data is information that relates to a living individual who can be either:

- Identified from that data;

or

- Can be identified from the information combined with any other information that is in the possession of the person or organisation holding the information.

Basic personal data includes:

- Name
- Address
- Date of birth
- Telephone numbers
- Email addresses
- Online identifiers including cookies and IP addresses (new under GDPR)
- Bank account details

The Data Protection Act also identifies includes "sensitive personal data". Before processing any sensitive personal data Traverse must gain explicit consent from the individual.

Sensitive personal data includes racial or ethnic origin, physical or mental health conditions, offences or alleged offences, religious beliefs, and details regarding sexual orientation.

Data privacy encompasses other factors that could be used to identify an individual, such as their genetic, mental, economic, cultural or social identity.

Personal information must be:

- Processed fairly and lawfully and not processed unless specific conditions are met
- Obtained only for one or more specified and lawful purposes, and not processed further in any manner incompatible with that purpose or those purposes
- Adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Not kept for longer than is necessary
- Processed in accordance with the rights of data subjects under the Act
- Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage

- Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

As of 25 May 2018 (under GDPR) data must be:

- Lawful, fair and transparent – processed lawfully, fairly and in a transparent manner
- Limited – collected for the specified explicit and legitimate purposes and not further processed
- Minimised: Adequate, relevant and limited to what is necessary in relation to purposes for which processed
- Accurate and kept up to date
- Not kept for longer than necessary
- Kept securely

Traverse, through appropriate management and controls, will:

- Observe conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply checks to determine the length of time information is held
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR

These include:

- The right to be informed that processing is being undertaken
- The right of access to one's personal information
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information which is regarded as wrong information
- Appropriate technical and organisational security measures being taken to safeguard personal information
- Ensuring that personal information is not transferred abroad without suitable safeguards
- Treating people impartially and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Setting out clear procedures for responding to requests for information.

In addition, Traverse will ensure that:

- There is someone with specific responsibility for Data Protection.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows how to do so
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are clearly described
- A regular review and audit is made of the way personal information is held, managed and used
- Regular assessments of performance and compliance with handling personal information take place.

Information Security Incident Reporting

Objective

To ensure information security incidents, events and weaknesses associated with information systems are reported in a timely manner to contain an incident and prevent recurrence and to allow corrective and/or preventative action to be taken and improve the ISMS.

Scope

This policy covers all Traverse information systems and services, employees, contractors, and third parties, who use, access, handle process, transmit, store, archive or dispose of information or information systems within the scope of the ISMS.

Related documents

Non-conformance log

Responsibilities

The responsibilities for this policy lie with the Group Chief Executive, Board, HoDs, Risk Owners, staff, contractors and third party users of Traverse information systems and services.

Definitions

Information security incident

An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information or information systems and weaken or impair business operations.

Information security event

An information security event indicates that the security of an information system, service, or network may have been breached or compromised, violated or a safeguard may have failed.

Information security weaknesses

An information security weakness indicates vulnerability in an information system that could be exploited and compromise or harm business operations.

Requirements

1. If a breach or potential weakness is discovered the first action should be to carry out initial mitigation to contain the breach. Then:
2. All employees and contractors are responsible for reporting identified security incidents immediately to:

   - Marcus Clissold-Lesser (Data Protection Officer)
   - Joe Carpenter (Head of ICS)
   - (if related to one or more projects) the relevant Project Director(s)

This should be initially by whatever means is most practical – always backed up with an email. If any of the above parties are not available then any Traverse Director should also be included.

3. The parties above, led by the DPO will assess the situation and determine next steps. Early actions (within first 24 hours) will include:

   - Assess whether the matter constitutes a breach which fulfils criteria for reporting to the DPO. If yes, the matter must be reported within 72 hours
   - Assess exactly what has occurred, which individuals may be affected and in what way they may have been affected
   - Report back to the Client (if project-specific) this will usually take the form of an initial conversation between the Traverse Project Director and the Client representative. Ways forward to be agreed, possibly through subsequent conversations

4. If agreed that the matter should be reported to the ICO, report to be submitted by the DPO within the timescales
5. Carry out agreed actions to mitigate – may include informing individuals of information breach
6. Determine the underlying cause and mitigate for the future

After rectification the non-conformance log is to be updated.

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	£
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details)		
Revised Term/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 on

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

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	Contractor (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	Contractor	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
Microsoft Office	Traverse	Admin	46	N/A			
Askia	QA Research	research / analysis					

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY

[To be discussed at kick off meeting]