CareQuality Commission

www.cqc.org.uk

Contract (Short Form – Services)

Contract for the provision of Recruitment for Market Research, Fieldwork, Consultation and Engagement- Services A

Contract Reference CQC AM 184

February 2020

Contents

1 Interpretation 2

2 Priority of documents 9

3 Supply of Services 9

4 Term 10

5 Price, Payment and Recovery of Sums Due 10

6 Premises and equipment 11

7 Staff and Key Personnel 13

8 Assignment and sub-contracting 14

9 Intellectual Property Rights 15

10 Governance and Records 16

11 Confidentiality, Transparency and Publicity 16

12 Freedom of Information 18

13 Protection of Data 19

13A Security 20

14 Liability and Insurance 20

15 Force Majeure 22

16 Termination 22

17 Compliance 24

18 Prevention of Fraud, Corruption and Bribery 24

19 Dispute Resolution 25

20 General 26

21 Notices 28

22 Governing Law and Jurisdiction 29

23 TUPE 29

SCHEDULE 1 –SPECIFICATION 31

SCHEDULE 2 – PRICE 38

SCHEDULE 3 – TENDER RESPONSE ..... Error! Bookmark not defined.

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS 41

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN 43

SCHEDULE 6 – CHANGE CONTROL 96

SCHEDULE 7 – THIRD PARTY SOFTWARE 97

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY 99

THIS CONTRACT is dated 4th February of 2020

PARTIES

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

and

(2) **72 POINT LIMITED** of The Media Centre, Abbeywood Business Park, Emma-Chris Way, Bristol, BS34 7JU (**"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 to perform **Recruitment for Market Research, Fieldwork, Consultation and Engagement**

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 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;
"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;

"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;
"Contract Period"	shall mean the Term of the Contract;
"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;
"Contractor's Response"	means the document submitted by the Contractor to the Authority in response to the Authority's invitation to suppliers for formal offers to supply the Services appended hereto in Schedule 3;
"Contractor System"	means the information and communications technology system used by the Contractor in performing the Services including the Software, the Contractor Equipment and related cabling (but excluding the Authority System);
"Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer"	shall each have the same meaning given in the GDPR;
"Data	means (i) the GDPR, the LED and any applicable national

Protection Legislation	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;
"Data Subject Request"	means a request made by or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access his or her 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;
"Default"	means any breach of the obligations of the relevant Party (including abandonment of the Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of the Contract and in respect of which such Party is liable to the other;
"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*;
"Good Industry Practice"	means standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of

	undertaking under the same or similar circumstances;
"Information"	has the meaning given under section 84 of the FOIA;
"Joint Controllers"	means where two or more Controllers jointly determine the purposes and means of processing;
"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;
"LED"	means Law Enforcement Directive (*Directive (EU) 2016/680*)
"Loss"	means any losses, costs, price, expenses, interest, fees (including legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, price, fines, damages, destruction, adverse judgments, orders or other sanctions and the term "**Losses**" shall be construed accordingly;
"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;
"Price"	means the price (excluding any applicable VAT) payable to the Contractor by the Authority under the Contract, as set out in Schedule 3 for the full and proper performance by the Contractor of its obligations under the Contrat;
"Pricing Schedule"	means Schedule 3 containing details of the Price;
"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;
"Prohibited Act"	means: (a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; (b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with the Contract; (c) an offence: i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act; ii) under legislation or common law concerning fraudulent acts; or iii) the defrauding, attempting to defraud or conspiring to defraud the Authority; any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct has been carried out in the UK;
"Protective Measures"	means appropriate technical and organisational measures which include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule 5 (Security Requirements and Plan);
"Purchase Order	means the Authority's unique number relating to the supply of the Services by the Contractor to the Authority in accordance with the

Number"	terms of the Contract;
"Relevant Requirements"	means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010;
"Replacement Contractor"	means any third party supplier appointed by the Authority to supply any services which are substantially similar to any of the Services in substitution for any of the Services following the expiry, termination or partial termination 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;
"Security Plan"	means the Contractor's security plan prepared pursuant to paragraph 3 of Schedule 5 (Security Requirements and Plan), an outline of which is set out in an Appendix to Schedule 5;
"Security Policy Framework"	means the HMG Security Policy Framework (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf)
"Services"	means the services to be supplied by the Contractor to the Authority under the Contract as set out in Schedule 1;
"Specification"	means the specification for the Services (including as to quantity, description and quality) as specified in an appended here to 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–Contractor"	means a third party directly or indirectly contracted to the Contractor (irrespective of whether such person is an agent or company within the

same group of companies as the Contractor) whose services are used by the Contractor (either directly or indirectly) in connection with the provision of the Services, and **"Sub-Contract"** shall be construed accordingly;

"Sub-processor"	means any third Party appointed to process Personal Data on behalf of the Processor related to this Contract;
"Supplier 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;
"TUPE"	means the Transfer of Undertakings (Protection of Employment) Regulations 2006;
"VAT"	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
"Variation"	means a variation to the Specification, the Price or any of the terms and conditions of the Contract;
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

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

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

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

1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the 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 Price, 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 Price 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 **4th February 2020** and shall expire on **3rd February 2021**, 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 **12 Months** 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 Price, Payment and Recovery of Sums Due

5.1 The Price for the Services shall be as set out in Schedule 2 and shall be the full and exclusive remuneration of the Contractor in respect of the supply of the Services. Unless otherwise agreed in writing by the Authority, the Price 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 Schedule 2. 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 Supplier 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 Data

13.1 Authority Data

13.1.1 The Contractor shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

13.1.2 The Contractor shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Contractor of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

13.1.3 To the extent that Authority Data is held and/or Processed by the Contractor, the Contractor shall supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification.

13.1.4 The Contractor shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data.

13.1.5 The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored securely off-site. The Contractor shall ensure that such back-ups are made available to the Authority immediately upon request.

13.1.6 The Contractor shall ensure that any system on which the Contractor holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework.

13.1.7 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Contractor's Default so as to be unusable, the Authority may:

(a) require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data and the Contractor shall do so promptly; and/or

(b) itself restore or procure the restoration of Authority Data, and shall be repaid by the Contractor any reasonable expenses incurred in doing so.

13.1.8 If at any time the Contractor suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Contractor shall notify the Authority immediately and inform the Authority of the remedial action the Contractor proposes to take.

13.2 Personal Data

13.2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor.

13.2.2 The Parties agree that they will comply with the provisions on Processing, Personal Data and Data Subjects in Schedule 4 .

13.2.3 The Parties shall at all times comply with Data Protection Legislation.

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 Price 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 estimated yearly Price paid] or payable to the Contractor under this Contract [whichever is higher]; and

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 18.4 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 £80,000

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 £500k pounds (£500,000);

c) Professional indemnity with the minimum cover per claim of £500k pounds (£500,000);

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, 17, 18.4 and 20.11; 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 If the Authority terminates the Contract under this clause, the Authority shall make no further payments to the Contractor except for Services supplied by the Contractor prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority.

16.6 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, 16.7, 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.

16.7 Upon termination or expiry of the Contract, the Contractor shall:

16.7.1 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

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

16.7

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 o [redacted]

[Tel:]

[Email:] [redacted]

21.3.2 For the Contractor:

[Address:] The Media Centre, Abbeywood Business Park, Emma-Chris Way, Bristol, BS34 7JU

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

[To be completed as 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 .....

Position ..

SIGNED for and on behalf of **[the Contractor]**

ACTING BY, Signature ..... [redacted]

Name:

Position:

A DIRECTOR, IN T[redacted]

Signature of witnes[redacted]

Witness name: .....

Witness Address: ..

Witness Occupation

SCHEDULE 1 – INVITATION TO TENDER AND SPECIFICATION

Background/Preamble

The Care Quality Commission (CQC) is the independent regulator for health and social care services in England. We monitor, inspect and regulate services to make sure they meet fundamental standards of quality and safety and we publish what we find including performance ratings to help people choose care.

CQC has a legal duty to engage the public in the development of its work and public engagement and insight are integral to ensuring CQC delivers its purpose. It enables us to understand what matters to people who use services, consequently helping to build public trust. This empowers the public to make choices around services and know what they should expect in terms of quality of care. It also enables CQC to meet its statutory requirements as set out in the Health and Social Care Act 2008 (and amended in 2013).

More generally, all aspects of our business plan require us to make sure our key audiences understand and feel they have been engaged in our approach.

The contracts are an essential mechanism for meeting our targets in the 2019-2020 Engagement and Public engagement Business plans and support the delivery of the following objectives:

Transformation Activity:

- Building our capability and capacity to deliver change well
    - Developing an overarching plan for engaging audiences in CQC's strategic change programme
- Transforming Registration
    - Delivering coproduction and insight with external key audiences to drive change
    - Provide insight to support the delivery of a public friendly categorisation of services that helps people find information more easily.
- Enable CQC to become intelligence driven
    - Deliver coproduction and insight to drive Monitor Discovery and Alpha
    - Deliver coproduction and insight to support change in Share Your Experience services
- Deliver our programme of user focussed digital technology
    - Deliver coproduction and insight to develop new web services
- Define our role in whole system regulation
    - Develop an overview of how systems are approaching engagement with people who use services, stakeholders and staff
    - Explore how to get people's views and experiences of care into an integrated system.

BAU Activity:

- Insight Monitoring and Evaluation
  - Insight reporting
- Contract procurement 19/20
  - Procure and deliver a call down contract to enable flexible insight activity with the public
- Manage the contracts and channels to provide quantitative and qualitative feedback
- Ensure CQC generates insight from all its stakeholder groups

We currently outsource the recruitment of people representative of the population of England to take part in coproduction of CQC policies, strategies, methods and products. We also outsource the recruitment of specific communities to take part in user research. We do not have the capacity or reach to deliver this targeted recruitment in house, at scale.

We require a more flexible, service to meet the organisations' need for agile coproduction and user research with specific communities, to reach a wider audience, and to deliver value for money.

1 **Scope of Works**

We are looking to procure a Supplier with a proven track record to deliver targeted recruitment of individuals across England, that provides value for money.

The Supplier will have a specific skillset and an agile mechanism for recruiting individuals according to a brief from CQC, from a representative sample as well from specific communities to provide quality engagement with CQC, including people and community:

- Who have used a health care service in the past 6 months
- Who have accessibility needs.
- With experience of using adult social care.
- Who have experienced poor care
- Who are 65+ year olds
- With a long-term condition
- Learning disabled

The supplier will be required to be responsive, flexible and agile to meeting the organisation's need to recruit the right people at the right time and have multiple recruitment channels, including via local organisations and charities so that we can mitigate the risks of:

- Speaking to the same people for different pieces of engagement work
- Not being able to target specific groups
- Only engaging with people in one part of the community.

The CQC will engage by both digital and non-digital means with recruited individuals to provide insights that are valuable and take part in the coproduction and user research in relation to (but not limited to):

- CQC current and future regulatory model
- Developments and changes CQC are proposing to their policies, processes, strategies, practices, methods and products
- Specific health and social care topics, where they have direct experience, and/or they would be significantly impacted by it.

The Supplier will be responsible for the renumeration of individuals taking part in the engagement such as any incentives or involvement fees and expenses such as travel or subsistence costs.

All mechanisms for paying individuals must comply with HMRC guidance on tax-deductible benefits.

Additional requirements: Any information/material etc. needed from CQC in order to recruit individuals.

2 Outputs

We expect the supplier to provide **pre-engagement:**

- Readiness, time, delivery, quantities/quality.
- Robust and fully resourced solutions to recruiting individuals.
- Clear, fair and robust policies for people they intend to recruit of behalf of CQC.

We expect the supplier to provide **during engagement**:

- Recruit individuals from population groups as specified by CQC.

We expect the supplier to provide **post-engagement**:

- Pay individuals an involvement fee and any expenses incurred for participation on behalf of CQC.
- Regularly evaluate policies and processes with recruited individuals for quality improvement purposes.
- Manage the contracts and channels to provide quantitative and qualitative feedback.
- Insight Monitoring Evaluation and reporting.
- Ensure CQC generates insight from all its stakeholder groups.

3 Timescales/Volumes/Milestones

DESCRIPTION	TARGET DATE	ACTION TO ACHIEVE	REVIEW DATE
CQC to submit request for panel type	Day 0	CQC to write brief and email supplier	
Panel accepted/ survey sent	2 weeks from receipt of recruitment request	Supplier to use channels and screen people to ensure they are suitable according to the brief	
Supplier to invoice CQC at the end of each survey	Within 4 weeks of survey	Supplier sends invoice to CQC	

4 Authority Responsibilities

- CQC to appoint a contract manager to oversee the performance and liaise with / report to supplier contract manager on all matters relating to the contract.
- CQC to appoint a project lead to work and liaise with / report to project manager on all day to day activities relating to the contract.
- To provide clear briefs to the supplier on requests in a timely manner.
- To pay accurate and valid invoices in a timely manner.
- To hold performance reviews and contract management meetings on regular basis as agreed with the Supplier.

5 Supplier Responsibilities

- Appoint a contract manager to oversee the performance and liaise with / report to CQC's contract manager.
- Appoint a dedicated project manager, to act as key point of contact, to work and liaise with / report to CQC's project lead on all day to day activities relating to the contract.
- Attend any project meetings and problem-solving sessions regularly as agreed and required by CQC's contract manager / project lead.
- Provide regular updates / progress reports of delivery (the format and frequency of reporting will be agreed at the outset of the contract between the supplier and CQC, but it should cover overall progress against activity, volumes used, plan, risks to plan and mitigating actions, issues and escalations and project budget tracking).
- Provide monthly in arrears accurate and timely invoicing upon satisfactory delivery of required output.

6 Contract Management

- To meet all the requirements of CQC as detailed in the Specification (Section 2).
- Perform quality assurance on all aspects of the programme to meet agreed service levels. The supplier is required to ensure that there is sufficient personnel and other resources to deliver the work packages on time to the quality standards required and to budget.
- Identify opportunities for continuous improvement to the quality and efficiency of the delivery of the service.
- The selected supplier will be expected to attend a post contract review to consider whether the objectives of the contract were met; to review the benefits achieved; and to identify any lessons learnt for future developments of the project and Training sessions for users for knowledge transfer

7 Key Performance Indicators (KPI's)

A clear set of KPIs will be developed along with a detailed outline of the kind of services we will require, with agreed deadlines and quality standards to enable clear and robust management of any contract awarded.

We will review KPI's and quarterly reports and will hold a formal review after 3 months to determine whether this contract meets the recruitment needs of CQC effectively and efficiently. If we determine that there are improvements that could be made we will adopt these and review again in a further 3 months with the supplier. If KPI's and quarterly report continue to underperform we will call off the contract with a period of one-month notice.

KPIs to be applied to this contract are:

Indicator	Measured by	Reference Point or Target	Review Date
Project Plan The supplier is required to deliver outputs as per specification and defined in the project plan i.e. - recruit within agreed timelines to meet the deadlines agreed upon. - Provide the relevant information to the	Review Project plan - The timeliness of deliverables against key dates as agreed with CQC.	Provide a project plan within 1 week of contract sign off.	Two weeks of contract sign off.

recruited people - Screen participants to assess suitability - Seek to ensure no person is duplicated for activity unless specifically requested			
Meetings The supplier is required to attend all planned operational delivery, performance review, end of project review and contract management meetings, unless otherwise agreed with the Authority.	Full attendance at Performance review / contract meetings as agreed with CQC.	At least 99% at all time.	Agreed meeting date.
Customer Service - Working with CQC The supplier will be contactable to the Authority between the hours of 9am to 5pm Monday to Friday. To communicate regularly and answer queries promptly from CQC	Responding to requests and queries from CQC.	100% at all time.	Reply to queries within 24, hours, resolved within 72hours and A written response by no more than 3 working days
Invoicing Provide accurate and timely invoicing on monthly basis for work satisfactorily completed / achievement of milestones, monthly in arrears, or report and associated sections being completed on time with appropriate content.	Accurate and timely invoices, as specified and agreed with CQC.	At least 99% at all time.	3rd working day of the Monthly

Recruitment of specified groups/individuals	The ability to recruit the required number of individuals requested by CQC to fulfil the engagement need	At least 99% at all time.	Quarterly
Timeliness of recruitment	The ability to recruit individuals requested by CQC by specified timescales	At least 99% at all time.	Quarterly
To provide a quarterly summary of number of people we have recruited through the contract including audience segmentation and number of times we have engaged with people	Shows fulfilment of engagement need across all requests	At least 99% at all time.	Quarterly

8 Exit Strategy - Skills and Knowledge Transfer

The selected supplier will work closely with CQC staff as necessary to ensure transfer of skills and knowledge. The successful supplier must ensure that any learning and any development opportunities are documented and communicated to CQC.

The mechanism for the transfer of knowledge will be agreed with the CQC contract managers, e.g. facilitated during certain stages by basing the contractor's staff in CQC offices or regular update meetings or providing training and guidance that may be required for relevant staff.

This must not be restricted to the end of the contract period, but instead must occur regularly via the monthly or quarterly programme reports at the very least.

SCHEDULE 2 – PRICE

This contract will be a Call off contract with a maximum spend of £19,488 including VAT

COST ENVELOPE
£17,088 - £19,488 inclusive of VAT per year Please note this contract will be a call off contract.

SCHEDULE 3 – CONTRACTOR'S RESPONSE

Fixed price submission

Please detail fixed price for the work specified in Section 2 - Scope of Works:

All Prices excluding VAT

[redacted]

9c				
	TOTAL			412.00

The rates may be used prorate for any variation in quantity if required.

N.B. It would be impossible to represent England with so few as 100 people. The minimum England sample we'd ever use would be 500, giving an error margin of +/- 4.4%. OnePoll prefers to do 2,000 sample as its standard sample size.

Table A - Day Rate Card

Tenderers are requested to complete the Day Rate Card Table below, detailing the Day Rates for a range of roles which are anticipated to have involvement in the delivery of work packages under the contract.

The information provided in the Day Rate Card Table will be cross-referenced with each pricing table to ensure clarity and will also be applicable to any additional services that are required beyond the defined work packages.

[redacted]

[redacted]

Day = 7.5 hours excluding lunch.

[redacted]

[redacted]

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

ANNEX 1 – Data Processing Schedule

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

2. The contact details of the Processor's Data Protection Officer are: [redacted] **jo.garner@swns.com, The Media Centre, Abbeywood Business Park, Emma-Chris Way, Bristol, BS34 7JU**

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

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

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller, the Care Quality Commission and the Contractor is the Processor, who is unknown until the procurement process is finished.
Subject matter of the processing	We will process the data given about recruitees (for face to face engagement) to determine whether they are the correct fit for the people that we want to engage with on a particular piece of work We need to know if they are new to CQC for our KPI's and quality monitoring. This data will include name, contact details, location, demographic data and background.
Duration of the processing	From contract implementation to end- the call off nature means that we will be able to use it throughout the entirety of the year. This may equate to 2 times per month, for

	varying number of recruits depending on business needs. Data will be stored and processed from receiving the data. We will store the data for up to a year to ensure that the people we are getting from the recruiters are different thus ensuring we are engaging with new people.
Nature and purposes of the processing	The processor will screen people according to our person specification. When these people have been screened they will suggest who may be suitable for our engagement. We will then use the information the share with us to determine if the person is suitable for the work. Data will be shared with us via phone and online methods and will be stored securely at CQC. We will store data for up to a year to ensure that we are being offered different people for engagements
Type of personal data	The processor will share names, contact details (ie phone and email) and background information with us as well as other demographic data.
Categories of Data Subject	Members of the public who have signed up to be part of a recruitment platform or who have contact with charities that the recruiter works with.
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	What is done with the data will be determined in writing with the data processor once the contract is in place

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

Who are SWNS Media Group?

SWNS Media Group incorporates South West News Service Limited and 72 Point Limited *(known by and referred to in this document as "SWNS"). OnePoll is a trading style of 72 Point Limited.*

What is the purpose of this document?

SWNS is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you before, during and after your relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all members of the OnePoll panel.

SWNS is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to members of the OnePoll panel. This notice does not form part of any other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

Information we collect when you sign up to join the OnePoll panel:

First Name

Last Name

Email Address

Country you reside in

Nationality

Nearest City (list of 30 options)

Post code

Marital Status

Home Owner Status

Gender

Date of Birth

Occupation

Telephone Number

Number of Children

If children are under 18 we ask for date of birth and gender

Other information we collect from you

Newsletter Subscription Status
iPhone User or Not
Members System Status Active/Blocked
Last Login Date
Last IP Address

Paypal or bank details to make payments to you

As part of your application to be a panel member we may send you profile polls to gather additional information

These polls are broken down into the following areas – you have the right to not complete the profile polls – the information provided will determine your eligibility as a panel member for answering surveys:

Education

Social Media

General

Holidays

Automobile

Hobbies

Financial

Media

Mobile Technology

Shopping

Gaming

Medical

Occupation

We may also collect, store and use the following "special categories" of more sensitive personal information – a full list of the sensitive personal questions we may ask you to complete is shown as appendix 1 to the policy:

Marital Status

Religion

Sexual Preferences and Behaviour

Ethnicity

Motoring Convictions and Other Criminal History

Gambling History and Behaviour

Medical History

Mental Health

Health and Fitness

Political Views

Philosophical or Moral Beliefs

How is your personal information collected?

We collect personal information about panel members through the application and registration process on the OnePoll system and app and through your usage of the system, the completion of profile polls and other surveys. You may provide further information by e mail from time to time.

We will collect additional personal information during the course of your panel membership period.

How we will use information about you?

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you including the analysis of surveys that you respond to on the OnePoll site or app.

2. OnePoll provides consolidated information on the surveys completed by panel members to clients – OnePoll does not share individual data on you or your personal responses to a survey to a client.

3. Where we need to comply with a legal obligation.

4. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above (see The kind of information we hold about you) primarily to allow us to perform our contract with you to provide appropriate surveys for you to answer in order for us to provide anonymised summary survey information for our client base. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. Making a decision about appropriate surveys for you to answer.

- Managing our contractual relationship
- Ensuring you are eligible to answer surveys for us.
- Paying you and accumulating credit on your account for future payment for the surveys that you have answered.
- To prevent fraud.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing you with surveys to answer), or we may be prevented from complying with our legal obligations.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type

of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we take special measures to ensure that personal information is anonymised

3. Surveys using special information are authorised in advance by a manager in the business

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where it is necessary to perform the contract with you such as selecting members eligible to answer a survey or analysing the results of a survey

2. In other limited circumstances, with your explicit consent and where appropriate measures are in place to safeguard your rights.

Data sharing

We will not share your personal information with third parties.

We provide survey results to our clients in summary format where raw data is provided to clients all personally identifiable information is removed.

Transferring information outside the EU

We will not transfer the personal information we collect about you outside the EU in order to perform our contract with you.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will

only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from our Panel and Community Manager.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you

If you do not log in to the OnePoll system for a period of 12 months your account is deactivated and your personal data is deleted. Survey responses that you have given in the past will be anonymised and identifiable only as a user number.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep your profile up to date and inform us if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove

your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Panel and Community Manager

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Panel and Community Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data protection officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at

any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Panel and Community Manager.

By registering as a panel member you acknowledge receipt of this policy and accept its terms.

Appendix 1 - Detailed List of Special Category Information we may request from you as part of our profile polling process:

GENERAL

Which of the following best describes your ethnicity?
White – British
White – Irish
White – Other
Black or Black British – Caribbean
Black or Black British – African
Black or Black British – Other
Asian or Asian British – Indian
Asian or Asian British – Pakistani
Asian or Asian British – Bangladeshi
Asian or Asian British – Other
Chinese or Other Ethnic Group – Chinese
Chinese or Other Ethnic Group – Other
Mixed
Other
Prefer not to say

What is your religion?
Christianity
Islam
Catholic
Hinduism
Buddhism
Sikhism
Judaism
Other religion
No religion
I prefer not to say

What is your marital status?
Single
In a relationship
Cohabiting
Married
Separated
Divorced
Widowed
Other

Are you...?
Heterosexual
Homosexual
Bisexual
Other
Prefer not to say
Which of the following do you celebrate?
Please select all that apply
Eid
Diwali
Easter
Christmas
New years
Mother's day
Ramadan
Father's day
Valentine's Day
Shrove Tuesday
None of the above

AUTOMOBILE

Do you currently have any points on your licence?
Yes
No

Have you ever been caught by police/traffic police/etc. doing any of the following whilst driving?
Please select all that apply
Speeding
Running a red light
On your mobile phone
Without your seatbelt on
Drinking alcohol / being drunk / drink driving
Driving while under the influence of drugs
None of the above / Prefer not to say

HOBBIES

Do you ever gamble (including online gambling?) e.g. Lotto, sports betting, Bingo

Yes online only
Yes but not online
Yes both online and offline
I don't ever gamble

What types of online gambling do you partake in?
Please select all that apply

Poker
Casino
Sports betting
Bingo
Lotteries
Other

How often on average do you gamble online? Please select best match

Every day
Every week
Once a fortnight
Once a month
Once every few months
Twice a year
Once a year
Less than once a year

MEDICAL

Which of the following health and medical issues/conditions/etc. do you CURRENTLY have?
Please select all that apply

Acute pain
Allergies
Breathing/Respiratory conditions
Chronic fatigue syndrome (CFS)
Cancer
Diabetes
Digestive conditions
Eye, ear, nose, throat conditions
Heart/Blood conditions
Immunological conditions
Mental health and Behaviour
Neurological/Brain-related conditions
Pain or bone/joint/muscle conditions
Physical appearance issues (i.e. hair loss, cosmetic appearance, etc.)
Sexual health problems
Skin condition
Sleep disorders
Weight condition
None of the above
None / Prefer not to say

Which of the following best describes you?

I have never had cancer

I have had cancer in the past
I currently have cancer
Prefer not to say
Which of the following cancers have you ever had / do you currently have?
Please select all that apply
Bladder
Bone
Brain
Breast
Cervical
Colon
Hodgkin's disease
Kidney
Leukemia
Liver
Lung
Melanoma
Non-Hodgkin's lymphoma
Ovarian
Prostate
Uterine/Cervical
Other cancer
Prefer not to say
Which of the following diabetes conditions currently affect you?
Please select all that apply
Type I Diabetes
Type II Diabetes
None of the above
None / Prefer not to say
Which of the following digestive conditions have ever affected you?
Please select all that apply
Bowel incontinence
Colitis
Constipation (Persistent or chronic)
Crohn's disease
Diarrhoea (Persistent or chronic)
Gall stones
Gas/Bloating
Heartburn/GERD
Inflammatory bowel disease (IBD)
Intestinal ulcers
Irritable bowel syndrome (IBS)
Kidney stones
Nausea
Overactive bladder
Stomach ulcers
Urinary incontinence/Bladder control issues
Urinary tract infection
Other gastrointestinal condition
None / No digestive conditions
None / Prefer not to say
Which of the following eye, ear, nose, and throat conditions have ever affected you?
Please select all that apply
Astigmatism

Blindness
Dry eye
Ear disorder, any
Ear infections
Eye infection
Glaucoma
Hearing loss
Hyperopia/Farsightedness
Macular degeneration
Myopia/Short-sightedness
Nasal congestion
Mouth ulcers
Nystagmus
Snoring
Vision correction-laser treatment
Vision impaired
Other ear, nose, throat condition
None / No eye, ear, nose, and throat conditions
None / Prefer not to say

Which of the following heart/blood conditions have ever affected you?
Please select all that apply

Abnormal heart rate
Angina
Blood transfusion
Circulation problem in the legs
Congestive heart failure (CHF)
Heart attack/Myocardial Infarction
Heart disease
Hemophilia or other blood disease
Hepatitis A
Hepatitis B
Hepatitis C
High blood pressure/Hypertension
High cholesterol
High triglycerides
Hyperlipidemia
Hypoglycemics
Low blood pressure/Hypotension
Stroke/TIA
Thrombosis
Varicose veins
Other heart/blood condition
None / No heart/blood conditions
None / Prefer not to say

Are you male or female?

Male
Female

Which of the following male related health conditions have ever affected you?
Please select all that apply

Ejaculation disorder (Premature ejaculation)
Erectile dysfunction/Impotence
Testes disorder
Other men's health condition
None / No men's health conditions
None / Prefer not to say

Which of the following women's health conditions have ever affected you?
Please select all that apply
Abnormal bleeding
Absence of periods
Endometriosis
Fibroids
Menstrual cramps (Dysmenorrhea)
Painful ovulation (Mittelschermz)
Pelvic inflammatory disease
Polycystic ovary syndrome (PCOS)
Premenstrual dysphoric disorder
Premenstrual syndrome (PMS)
Thrush / Candida/Yeast infection
Vaginal infections, e.g. bacterial vaginosis
Other women's health condition
None / No women's health conditions
None / Prefer not to say
Which of the following best describes you?
I am not pregnant but have not yet been through the menopause
I am currently pregnant
I am currently going through the menopause and have used HRT
I am currently going through the menopause and have not used HRT
I have been through the menopause and have used HRT
I have been through the menopause and have not used HRT
Prefer not to say
Which of the following mental health or behavioural conditions have ever affected you?
Please select all that apply
Anxiety
Attention deficit (ADHD, ADD)
Bipolar (Manic depression)
Chronic depression (Dysthymia)
Clinical depression/Major depressive disorder
Dementia
Eating disorder
Obsessive compulsive disorder (OCD)
Panic attacks
Phobias
Post traumatic stress disorder (PTSD)
Psychiatric disorders
Seasonal depression (Seasonal affective disorder: SAD)
Social anxiety disorder
Stress anxiety
Other mental health or behavioural condition
None / No mental health or behavioural conditions
None / Prefer not to say
Which of the following neurological/brain-related conditions have ever affected you?
Please select all that apply
Alzheimer's
Dementia
Epilepsy
Multiple Sclerosis (MS)
Myalgic Encephalopathy (ME)
Parkinson's

Persistent tremor
Seizures (unrelated to epilepsy)
Stroke (TIA)
Other brain/Neurological condition
None / No neurological/brain-related conditions
None / Prefer not to say
Do you currently use contraceptives?
Yes - barrier methods only (e.g. condom, diaphragm)
Yes - other contraceptive methods only (e.g. contraceptive pill, coil, vasectomy)
Yes - both barrier methods and other contraceptive methods
No
Prefer not to say
Which of the following barrier method contraceptives do you or your partner currently use?
Please select all that apply
Male condom
Female condom/Femidom
Cervical cap (with spermicide)
Cervical shield
Diaphragm (with spermicide)
Spermicidal foam
Sponge (with spermicide)
Other barrier method
None / Prefer not to say
Which of the following contraceptives do you (or your partner, if not applicable to you) currently use?
Combined oral contraceptive pill
Progesterone only pill (mini-pill)
Coil/IUD
Contraceptive patch
Injection
Implant
Sterilisation (vasectomy, tubal litigation, etc.)
Other contraceptive method
Prefer not to say
Which of the following sexual health conditions have ever affected you?
Please select all that apply
Chlamydia
Gonorrhea
Syphilis
Thrush / Candida/Yeast infection
Genital warts/Genital herpes
Human papilloma virus (HPV)
HIV/AIDS
Impotence
Infertility
Lack of sexual desire
Sexual dysfunction
Other sexually transmitted diseases (STD)'s
Other sexual health condition
None / No sexual health conditions
None / Prefer not to say
Which of the following skin conditions have ever affected you?
Please select all that apply
Acne

Age spots
Amyloidosis
Dandruff
Dry skin
Eczema
Fungal infections
Moles/ Warts
Psoriasis
Rosacea
Scleroderma
Skin Rash (Dermatitis)
Varicose veins
Other skin condition
None / No skin conditions
None / Prefer not to say

Which of the following sleep disorders or conditions have ever affected you? Please select all that apply

Insomnia
Narcolepsy
Snoring
Restless leg syndrome
Sleep apnoea
Sleep walking
Other sleep disorder or condition
None / No sleep disorders or conditions
None / Prefer not to say

Which of the following BMI/weight categories do you fall into? If you are unsure, please estimate.

Obesity (BMI of 30+)
Overweight (BMI of 25-29.9)
Normal weight (BMI of 18.5-24.9)
Underweight (BMI of less than 18.5)
Prefer not to say / don't know

Which of the following medical devices have you EVER used?

Please select all that apply
Reading glasses
Retainers
Stent
Walker
Wheelchair
Blood glucose meter
Braces
Cane
Contact lenses
Crutches
Dentures
Epipen
False teeth
Hearing Aids
Hip replacement
Inhalers
Insulin injections
Mouthguard
Nebulizers
Nicotine gum

Nicotine patches
Oxygen tanks
Pacemakers
Prescription eyeglasses
Prosthetic device
None of these medical devices
None / Prefer not to say
Which of the following medical devices to you CURRENTLY use?
Please select all that apply
Reading glasses
Retainers
Stent
Walker
Wheelchair
Blood glucose meter
Braces
Cane
Contact lenses
Crutches
Dentures
Epipen
False teeth
Hearing Aids
Hip replacement
Inhalers
Insulin injections
Mouthguard
Nebulizers
Nicotine gum
Nicotine patches
Oxygen tanks
Pacemakers
Prescription eyeglasses
Prosthetic device
None of these medical devices
None / Prefer not to say
Which of the following statements do you agree with?
Please select all that apply
I have dyslexia
I have been hospitalised
I have had hives
I have gone into anaphylactic shock
None of the above / Prefer not to say
Which of the following health and medical issues/conditions/etc. have ever affected one of your close family members/friends?
Please select all that apply
Acute pain
Allergies
Breathing/Respiratory conditions
Cancer
Diabetes
Digestive conditions
Eye, ear, nose, throat conditions
Heart/Blood conditions
Immunological conditions

Men's health problems
Mental health and Behaviour
Neurological/Brain-related conditions
Pain or bone/joint/muscle conditions
Physical appearance issues (i.e. hair loss, cosmetic appearance, etc.)
Sexual health conditions
Skin condition
Sleep disorders
Weight condition
Women's health problems
None of the above / None that I know of / Prefer not to say

VERSION 0.1

JUNE 4, 2018

SWNS AND 72POINT IT SECURITY POLICY

PRESENTED BY: JAMES MILLARD

SWNS LTD\72POINT LTD
THE MEDIA CENTRE UNIT A, EMMA CHRIS WAY, FILTON ABBEY WOOD, BRISTOL, BS34 7JU

IT SECURITY POLICY

ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Security Officers	James Millard, Azic Razzak
Board	Paul Walters, Chris White, Andrew Young, Martin Winter, Chris Pharo.

EMPLOYEES SECURITY

Employees are responsible for keeping their password secure. E.g. Not sharing passwords, Writing passwords on sticky notes and leaving in plain sight e.g. stuck to monitor.

Company computers must be locked at the screen whilst the member of staff is away from the computer for any period. A default domain policy is set to 15 minutes of inactivity.

Employees must use a complex password got company systems, with a minimum of 8 characters in length and use 3 of the 4 requirements which are upper case, lower case, number or special character. Common simple passwords are not advised such as Password1234 or P@55w0rd, etc

IT's recommendation is not to use the same password for everything, however a few complex passwords is recommended over different systems. Example: Keep your banking and email passwords separate should one be compromised.

Employees working documents should be stored on their company cloud drives, or network drives for security and redundancy.

Employees should also be aware of the dangers of social engineering and challenge anybody they notice that they do not recognize working within sanative areas. E.g. BT engineers which are unscheduled or anyone wishing to connect to SWNS\72Point resources remotely. Please challenge or contact the IT team if in doubt.

When working from remote locations it's recommended to only send company information only over approved sites or through encrypted methods, most commonly identified with https.

EMPLOYEES COMPUTERS

Employee's computers are required to have an up to date antivirus software, which will notify any risks, or threats and updating automatically on a regular bases. This is deployed when equipment is being provisioned however if the employee notices a warning, they should report to IT so it can be cleared or resolved.

Employee's computers are protected via a BIOS or Hard drive security, with encryption being an added benefit where possible, this cannot be removed for security purposes.

Bitlocker encryption keys will be stored in active directory and during issues may be required to trouble shoot the computer, however this may wait until addition software is in place. Again these will be deployed by the IT team, but please do not share passwords for power on or hard drive security with non SWNS\72Point employees.

COMPANY SECURITY

All physical machines must remain up to date with security updates, have an up to date antivirus software installed and running. The IT team manages these and updates and they should be installed when prompted.

(If the employee is prompted first thing in the morning, it is recommended they restart the computer at the end of the day)

Company owned assets assigned to individuals, with the responsibility being held with the employee for the device. If lost/stolen IT must be informed immediately where there may be a cost involved to the employee. Costs will be back on the deprecation value of the equipment, however stolen from a locked office whilst secured away should be covered by the SWNS insurance policy.

Company data that needs to be transferred\transported via USB or Hard drive must store securely, where Encrypted drives are highly recommended. A minimum of securely encrypted files, if there is a requirement to store on a non-encrypted drives. Only transporting the minimum amount of data required.

Backups taken from appliances\systems, which may contain company sensitive data must be stored securely and encrypted if being taken off site.

When disposing of equipment where data has been stored drives are to be removed and destroyed correctly, these can be stored securely until there is a significant number then can be shredded with a recorded of each of the drives being destroyed or wiped to info sec standards.

Drives can also be erased using the British HMG Infosec Standard 5, Enhanced Standard which performs a low level writes to disk combined with a previously encrypted drive is the minimal requirement for disposal.

Penetration Testing

Internal tests and scans to be completed quarterly of all externally facing servers. This is to monitored and reviewed each time for improvements and future proofing.

SWNS will also arrange for an external penetration test of all area's of the organization from an external attack point, this will be looking for vulneracilities in web applications and external security including wireless networks.

BUSINESS CONTINUITY MEASURES

BUSINESS CONTINUITY AND BACKUPS

Backups

Backups are moving to a server using Acronis software, these backups are responsible for backing up the Hyper-V hosts which are running the live VM's.

This will hold a daily incremental backup with a weekly full backup, retention policy will originate at 60 days onsite with a monthly or quarterly backup taken off site.

Backups will be stored in a snap shot view to ensure files and folders can be recovered for any issue including Ransomware.

Systems hosted by data centers such as UK Fast or Digital Ocean. An onsite team manages the hardware and the IT team restricts access.

Business Continuity

Security on the environment will follow the same guidelines where cloud hosted* and on premise apply. External access will be restricted to the essential ports required for that service to run. *Cloud hosted servers will have RDP\SSH access disabled by default, however will be enabled when required to access or modify the server.

OnePoll and CMS systems are backed up however business continuity is being worked on for the Q4 2019 where we will look to run a parallel system in a low performance model so systems are replicated on an almost real-time system.

Internal servers will be backed up in the Bristol office however an offsite copy will be available in our Birmingham office.

OFFSITE DATA STORAGE

Any data which is stored outside of SWNS Media group offices must be encrypted at rest and only accessible with approved authentication methods.

Data hosted with providers must have approved managed access measures and encrypted and drives removed from server hardware must go through approved disposal measures such as wiping to British HMG Infosec Standard 5, Enhanced Standard or hard drive onsite shredding.

Documentation must be provided in both instances for confirmation that hard drives have been destroyed to the correct standards required.

BRING YOUR OWN DEVICE (BYOD)

Employees may have the requirement to use their personal devices in the work place. This can be for a variety of reasons.

Employees are allowed to access resources which are available through a web browser based resources whilst working remotely on personal devices however it is recommend to remain vigilant about what is downloaded to your personal devices. E.g. Downloading a client list to your home laptop to work on where your laptop is stolen you may be liable for the information lost.

Use of personal equipment within the internal network is allowed and will require permission from your line manager with a requirement from IT to check the device to ensure that is has the latest updates and a working Antivirus software.

Data is only to be transported or transmitted through a secure methods, data held on laptops need to have a level of encryption to ensure the device is secure should it be lost or compromised.

In order to use your personal mobile device to access work emails and resources, employee's maybe asked to install a mobile device management tool this will allow IT to remotely remove or wipe mobile devices should they be lost/stolen or in the event the employee is exited from the company. This is targeted towards the business content on the device, however should there be an issue clearing we reserve the right to complete a full remote wipe.

Information Security Policy

72 Point Ltd/SWNS Ltd

(Company Name)

1st Dec 2017

(Date)

Contents

Introduction 78

Information Security Policy 78

1. Network Security 79
2. Acceptable Use Policy 79
3. Protect Stored Data 80
4. Information Classification 80
5. Access to the Sensitive Cardholder Data 81
6. Physical Security 81
7. Protect Data in Transit 82
8. Disposal of Stored Data 82
9. Security Awareness and Procedures 83
10. Credit Card (PCI) Security Incident Response Plan 83
11. Transfer of Sensitive Information Policy 89
12. User Access Management 90
13. Access Control Policy 91

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies 93

Appendix B – List of Devices 94

Introduction

This Policy document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and fully understand this policy. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and re-distributed to all employees and contractors where applicable.

Information Security Policy

72 Point Ltd/SWNS Ltd handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

72 Point Ltd/SWNS Ltd commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity and classification;
- Limit personal use of 72 Point Ltd/SWNS Ltd information and telecommunication systems and ensure it doesn't interfere with your job performance;
- 72 Point Ltd/SWNS Ltd reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;

- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

1. Network Security

A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

In addition, ASV should be performed and completed by a PCI SSC Approved Scanning Vendor, where applicable. Evidence of these scans should be maintained for a period of 18 months.

2. Acceptable Use Policy

Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to 72 Point Ltd/SWNS Ltd's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions, either knowingly or unknowingly by individuals. 72 Point Ltd/SWNS Ltd will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- The List of Devices in Appendix B will be regularly updated when devices are modified, added or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution of devices.

- Users should be trained in the ability to identify any suspicious behaviour where any tampering or substitution may be performed. Any suspicious behaviour will be reported accordingly.
- Information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of 72 Point Ltd/SWNS Ltd, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3. Protect Stored Data

- All sensitive cardholder data stored and handled by 72 Point Ltd/SWNS Ltd and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by 72 Point Ltd/SWNS Ltd for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

1. **The contents of the payment card magnetic stripe (track data) on any media whatsoever.**
2. **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
3. **The PIN or the encrypted PIN Block under any circumstance.**

4. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to 72 Point Ltd/SWNS Ltd if disclosed or modified. **Confidential data includes cardholder data.**
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure.
- **Public data** is information that may be freely disseminated.

5. Access to the Sensitive Cardholder Data

All Access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix C.
- 72 Point Ltd/SWNS Ltd will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- 72 Point Ltd/SWNS Ltd will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.
- The Company will have a process in place to monitor the PCI DSS compliance status of the Service provider.

6. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on 72 Point Ltd/SWNS Ltd sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces are periodically inspected to detect tampering or substitution.

- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of and=y third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel. 72 Point Ltd/SWNS Ltd sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

7. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

8. Disposal of Stored Data

- All data must be securely disposed of when no longer required by 72 Point Ltd/SWNS Ltd, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- 72 Point Ltd/SWNS Ltd will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- 72 Point Ltd/SWNS Ltd will have documented procedures for the destruction of electronic media. These will require:

- All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
- If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

9. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Company.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

10. Credit Card (PCI) Security Incident Response Plan

- 72 Point Ltd/SWNS Ltd PCI Security Incident Response Team (PCI Response Team) is comprised of the Information Security Officer and Merchant Services. 72 Point Ltd/SWNS Ltd PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. That member of the team receiving the report will advise the PCI Response Team of the incident.

3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

72 Point Ltd/SWNS Ltd PCI Security Incident Response Team (or equivalent in your organisation):

CIO

Communications Director

Compliance Officer

Counsel

Information Security Officer

Collections & Merchant Services

Risk Manager

Information Security PCI Incident Response Procedures:

- A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform 72 Point Ltd/SWNS Ltd PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

Incident Response Notification

Escalation Members (or equivalent in your company):

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyze the logs and related information from various central and local safeguards and security controls
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See below for these requirements.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary

   a. Include overview of the incident
   b. Include RISK Level(High, Medium, Low)
   c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures

   a. Include forensic tools used during investigation

V. Findings

   a. Number of accounts at risk, identify those stores and compromised

   b. Type of account information at risk
   c. Identify ALL systems analyzed. Include the following:

      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)

   d. Identify ALL compromised systems. Include the following:

      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)

   e. Timeframe of compromise

   f. Any data exported by intruder
   g. Establish how and source of compromise
   h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
   i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of the company will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

I. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers
IV. Obtain additional specific requirements from Discover Card

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

11. Transfer of Sensitive Information Policy

- All third-party companies providing critical services to 72 Point Ltd/SWNS Ltd must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with the Company's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must

1. Adhere to the PCI DSS security requirements.
2. Acknowledge their responsibility for securing the Card Holder data.

3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

12. User Access Management

- Access to 72 Point Ltd/SWNS Ltd is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

  Name of person making request;
  Job title of the newcomers and workgroup;
  Start date;
  Services required (default services are: MS Outlook, MS Office and Internet access).

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all 72 Point Ltd/SWNS Ltd systems is provided by IT and can only be started after proper procedures are completed.

- As soon as an individual leaves 72 Point Ltd/SWNS Ltd employment, all his/her system logons must be immediately revoked.

- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

13. Access Control Policy

- Access Control systems are in place to protect the interests of all users of 72 Point Ltd/SWNS Ltd computer systems by providing a safe, secure and readily accessible environment in which to work.
- 72 Point Ltd/SWNS Ltd will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to 72 Point Ltd/SWNS Ltd CISO.
- Access to 72 Point Ltd/SWNS Ltd IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any 72 Point Ltd/SWNS Ltd IT resources and services will be provided without prior authentication and authorization of a user's 72 Point Ltd/SWNS Ltd Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined

by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.

- Users are expected to become familiar with and abide by 72 Point Ltd/SWNS Ltd policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

Employee Name (printed)

Department

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

Employee Signature

Date

Appendix B – List of Devices

Asset/Device Name	Description	Owner/Approved User	Location

Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date

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?
QuestionPro survey software							

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY

To be discussed at kick off meeting