www.cqc.org.uk

Contract (Short Form – Services)

Contract for the provision of Transformation Communications Support

Contract Reference: CQC AM 174

October 2019

Contents

THIS CONTRACT is dated 7th October of 2019

PARTIES

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

and

(2) **REDHOUSE LANE COMMUNICATIONS LIMITED** of 1 Sans Walk, London, EC1R 0LT, Company Number: 2320395 (**"Contractor"**)

(Together the **"Parties"**)

Background

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

2. In order of the provision of Transformation Communication Support.

3. The Contractor has been appointed by the Authority to provide the Services.

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

1 Interpretation

1.1 In these terms and conditions:

"Approval"	means the written consent of the Authority;
"Authority"	means the Care Quality Commission;
"Authority Data"	means: (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Authority; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to the Contract; or (b) any Personal Data for which the Authority is the Data Controller;
"Award Letter"	means the letter from the Authority to the Contractor containing these terms and conditions;
"Anti-Slavery and Human Trafficking Laws"	means all applicable anti-slavery and human trafficking laws, statutes, regulations, policies and codes from time to time in force including but not limited to the Modern Slavery Act 2015;
"Breach of Security"	means any incident that result in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms;
"Central Government Body"	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or

	(d) Executive Agency;
“Charges”	means the charges for the Services as specified in the Schedule 2;
“Change Control Notice (“CCN”)”	means a change control notice in the form set out in Schedule 6;
“Contract”	means the contract consisting of these terms and conditions, any attached Schedules, the invitation to tender including Specification, the Tender Response and Award Letter between the Authority the Contractor;
“Confidential Information”	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
“Contractor”	means the person named as Contractor who was awarded this contract;
“Data Controller, Data Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer”	shall each have the same meaning given in the GDPR;
“Data Protection Legislation	means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to the processing of Personal Data and privacy; (iii) all applicable Law about the processing of Personal Data and privacy;
“Data Loss Event”	means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;

“DPA”	means the Data Protection Act 2018 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such legislation;
“Expiry Date”	means the date for expiry of the Contract as set out in the Award Letter;
“FOIA”	means the Freedom of Information Act 2000;
“GDPR”	means the General Data Protection Regulation (*Regulation (EU) 2016/679*;
“Information”	has the meaning given under section 84 of the FOIA;
“Key Personnel”	means any persons specified as such in the Specification or Contract otherwise notified as such by the Authority to the Contractor in writing;
“Law”	means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply;
“Loss”	means any losses, costs, charges, expenses, interest, fees (including legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, charges, fines, damages, destruction, adverse judgments, orders or other sanctions and the term “**Losses**” shall be construed accordingly;
“LED”	means Law Enforcement Directive (*Directive (EU) 2016/680*)
“Party”	means the Contractor or the Authority (as appropriate) and “Parties” shall mean both of them;
“Premises”	means the location where the Services are to be supplied, as set out in the Specification;
“Processing”	has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted accordingly;
“Processor	means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the

Personnel”	performance of its obligations under this Contract;
“Protective Measures”	means appropriate technical and organisational measures which include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule 5 (Security Requirements and Plan);
“Purchase Order Number”	means the Authority’s unique number relating to the supply of the Services by the Contractor to the Authority in accordance with the terms of the Contract;
“Request for Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Schedule”	means a schedule attached to, and forming part of, the Contract;
“Services”	means the services to be supplied by the Contractor to the Authority under the Contract;
“Specification”	means the specification for the Services (including as to quantity, description and quality) as specified in the Award Letter and appended hereto in Schedule 1;
“Staff”	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor engaged in the performance of the Contractor’s obligations under the Contract;
“Staff Vetting Procedures”	means vetting procedures that accord with good industry practice or, where requested by the Authority, the Authority’s procedures for the vetting of personnel as provided to the Contractor from time to time;
“Sub-processor”	means any third Party appointed to process Personal Data on behalf of the Processor related to this Contract;
“Contractor Code of Conduct”	means the HM Government Contractor Code of Conduct dated September 2017;
“Term”	means the period from the start date of the Contract set out in the Award Letter to the Expiry Date as such period may be extended in accordance

with clause 4.2 or terminated in accordance with the terms and conditions of the Contract;

"Third Party Software"	means software which is proprietary to any third party which is or will be used by the Contractor to provide the Services including the software and which is specified as such in Schedule 7;
"VAT"	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
"Variation"	means a variation to the Specification, the Charges or any of the terms and conditions of the Contract;
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

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

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

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

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

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

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

2 Priority of documents

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

a) these terms and conditions

b) the Schedules

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

3 Supply of Services

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

3.2 In supplying the Services, the Contractor shall:

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

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

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

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

3.2.5 comply with all applicable laws; and

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

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

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

4 Term

4.1 The Contract shall take effect on the 7th October 2019 and shall expire on the 6th October 2020, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.

4.2 The Authority may extend the Contract for a period of up to 2 years with an annual review by giving not less than 10 Working Days' notice in writing to the Contractor prior to the Expiry Date. The terms and conditions of the Contract shall apply throughout any such extended period.

5 Charges, Payment and Recovery of Sums Due

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

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

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

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

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

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

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

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

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

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

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

6 Premises and equipment

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

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

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

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

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

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

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

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

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

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

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

7 Staff and Key Personnel

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

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

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

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

and the Contractor shall comply with any such notice.

7.2 The Contractor shall:

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

7.2.2 if requested, provide the Authority with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Authority's premises in connection with the Contract;

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

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

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

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

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

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

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

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

8 Assignment and sub-contracting

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

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

8.3 If the Authority has consented to the placing of Sub-Contracts, the Contractor shall:

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

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

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

9 Intellectual Property Rights

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

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

9.3 The Contractor hereby grants the Authority:

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

9.3.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

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

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

including any modifications to or derivative versions of any such intellectual property rights, which the Authority reasonably requires in order to exercise its rights and take the benefit of the Contract including the Services provided.

9.4 The Contractor shall indemnify, and keep indemnified, the Authority in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded

against or incurred or paid by the Authority as a result of or in connection with any claim made against the Authority for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Contractor its Staff, agents or sub-contractors.

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

10 Governance and Records

10.1 The Contractor shall:

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

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

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

11 Confidentiality, Transparency and Publicity

11.1 Subject to clause 11.2, each Party shall:

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

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

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

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

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

11.2.3 on a confidential basis, to its professional advisers;

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

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

11.2.6 where the receiving Party is the Authority:

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

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

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

d) in accordance with clause 12.

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

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

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

12 Freedom of Information

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

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

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

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

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

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

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

13 Protection of Personal Data

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

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

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

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

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

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

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

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

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

(b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

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

(c) ensure that:

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

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

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

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

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

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

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

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

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

13.5 Subject to clause 13.6, the Processor shall notify the Controller immediately if it:

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

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

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

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

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

(a) the Controller determines that the processing is not occasional;

(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

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

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

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

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

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

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

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

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

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

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

13A Security

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

13A.2 The Contractor shall ensure that the Security Plan produced by the Contractor fully complies with Schedule 5 (Security Requirements and Plan).

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

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

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

13A.6 The Contractor shall be liable for, and shall indemnify the Authority against all Losses suffered or incurred by the Authority and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of Security (to the extent that such Losses were not caused by any act or omission by the Authority).

14 Liability and Insurance

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

14.2 Subject always to clauses 14.3, 14.4 and 14.5:

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

14.2.2 except in the case of claims arising under clauses 9.4 and 18.4, in no event shall the Contractor be liable to the Authority for any:

a) loss of profits;

b) loss of business;

c) loss of revenue;

d) loss of or damage to goodwill;

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

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

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

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

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

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

14.4 The Contractor's liability under the indemnity in clauses 9.4 and 18.3 shall be unlimited.

14.5 The Contractor's liability for all Losses suffered or incurred by the Authority arising from the Contractor's Default resulting in the destruction, corruption, degradation or damage to Authority Data or Personal Data or any copy of such Authority Data or Personal Data shall in no event exceed fifty thousand pounds (£50,000).

14.6 The Contractor shall hold:

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

b) Public liability with the minimum cover per claim of five million pounds (£5,000,000);

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

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

15 Force Majeure

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

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

16 Termination

16.1 The Authority may terminate the Contract at any time by notice in writing to the Contractor to take effect on any date falling at least 1 month (or, if the Contract is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.

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

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

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

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

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

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

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

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

16.4 The Contractor may terminate the Contract by written notice to the Authority if the Authority has not paid any undisputed amounts within 90 days of them falling due.

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

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

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

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

17 Compliance

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

17.2 The Contractor shall:

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

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

17.3 The Contractor shall:

17.3.1 perform its obligations under the Contract in accordance with all applicable equality Law and the Authority's equality and diversity policy as provided to the Contractor from time to time; and

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

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

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

17.5.1 the Official Secrets Acts 1911 to 1989; and

17.5.2 section 182 of the Finance Act 1989.

18 Prevention of Fraud, Corruption and Bribery

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

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

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

18.2 The Contractor shall not during the Term:

18.2.1 commit a Prohibited Act; and/or

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

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

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

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

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

19 Dispute Resolution

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

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

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

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

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

20 General

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

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

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

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

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

20.4.2 terminate the Contract with immediate effect, except where the Contractor has already provided all or part of the Services or where the Contractor can show evidence of substantial work being carried out to fulfil the requirement of the Specification, and in such case the Parties shall attempt to agree upon a resolution to the matter. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at clause 19.

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

20.6 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Contract shall be valid only if it is communicated to the other Party in writing and

expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Contract.

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

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

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

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

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

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

21 Notices

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

21.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter (sent by hand, first class post, recorded delivery or special

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

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

21.3.1 For the Authority:

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

For the attention of: [redacted]

Tel: [redacted]

Email [redacted]

21.3.2 For the Contractor:

Address: 1 Sans Walk, London, EC1R 0LT

For the attention of: [redacted]

Tel [redacted]

Email: [redacted]

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

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

22 Governing Law and Jurisdiction

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

23 TUPE – NOT APPLICABLE

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

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

Signature ..[redacted]

Name .....

Position ....

SIGNED for and on behalf of **REDHOUSE LANE COMMUNICATIONS LTD**

Signature ..[redacted]

Name .....

Position ...

SCHEDULE 1 – Specification

The Requirement

Over the next five years, we are going to make it easier for us to do our job, make it easier for providers to work with us to do their job and make it easier the public to use what we know.

We need to bring this ambition to life for our people and external partners – helping them to understand why we are changing, what the future state looks like, how we will get there and how they can be part of that journey.

Outputs of the work:

1. Engagement narrative development

We want to develop a five-year change narrative that is owned and endorsed by our senior leadership team. We want to support this with creative content which helps the different audiences engage in the vision, including development of audience personas to support this thinking.

2. Developing creative campaigns and products

We would want the successful agency to support our evidence-based campaign plans with creative content on a call off basis for individual change programmes. We also want to create a visual identity for the transformation programme and projects within CQC's existing brand.

3. Iterative evaluation

We would want our partner agency to produce evaluation plans, measuring the quantifiable success of different content and amending the campaign delivery on an ongoing basis, based on levels of impact and achievement of outcomes.

CQC would also like the supplier to provide an evaluation following the end of each campaign delivery phase which covers the following:

- Which methods worked best for which audience;
- What content performed best with which audience;
- What method was the most successful overall;
- Success against the desired outcomes articulated below.

As part of the contract the successful supplier is expected to develop a methodology of tracking and evaluating outcomes as agreed with CQC for projects and overall for the programme of work. This methodology and the resulting outcomes should be shared with CQC for our own verification.

Expected outcomes:

Examples of the overall expected outcomes resulting from completion of this project are as follows:

- Improvements in colleagues' commitment to CQC's strategic direction
- A higher percentage of stakeholders feeling informed about the transformation programme (over 37% for internal stakeholders)
- A higher percentage of stakeholders feel they have had an opportunity influence the change (over 35% for internal colleagues)
- A higher percentage of stakeholders understanding why changes are being made (over 50% for internal colleagues) and feeling they have had an input (over 35% for internal colleagues)
- High adoption rates of new internal tools and services such e.g. O365
- Improved impact and reach of online communication products as measured by usage tools – hit rates etc. – measured against our current reach and impact levels
- Greater engagement with online content and more active participation in online discussions
- Internally improved feedback on our regular transformation briefing calls with leadership on change communication
- Externally improved feedback in our co-production and other provider events on their understanding of our transformation programme
- Externally improved feedback from the public on communication on new services

Key Performance Indicators

Indicator	Measured by	Reference Point or Target	Review Date
Once the rate card is agreed with CQC, the supplier will supply a project plan of confirmation setting an agreed timescale and costs for delivery	Delivery within 10 working days and sign off by CQC	Sign off meeting	3 months
Commencement of delivery against agreed plan, with iterative learnings applied as the campaign or product progresses	Ongoing pulse survey results improving	Regular review meetings during the project	3 months
Meeting the outcomes agreed with CQC for each project e.g. A higher	Surveys and feedback	Meeting agreed target percentage	3 months

percentage of stakeholders feeling informed about change		improvement	
Evaluation report (to include success of campaign/product against agreed objectives, lessons learned reflections from the supplier on what's worked well and what hasn't, that can be used for any future activity of this nature).	Report 10 days after campaign end/product launch	Within one month following the end of the campaign/product delivery phase	3 months

SCHEDULE 2 – CHARGES

Care Quality Commission want the successful agency to support our evidence-based campaign plans with creative content on a call off basis for individual change programmes. CQC also want to create a visual identity for the transformation programme and projects within CQC's existing brand.

Cost Envelope

Total contract value including VAT will be up to a maximum of **£95,000** per annum

Statement of Works

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

Once requirement have been determined, CQC will provide Redhouse Lane Communications Ltd with the document below.

Redhouse Lane Communications Ltd are required to complete the Statement of Works within a determined timeframe prior to any work commencing

Statement of Works

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

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

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

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

BY SIGNING AND RETURNING THIS ORDER FORM THE CONTRACTOR AGREES to enter a legally binding contract with the Authority to provide to the Customer the Services specified in the Order Form, incorporating the Care Quality Commission Terms set out in the agreement entered into by the Contractor and the Authority on **7th October 2019**.

For and on behalf of the Contractor:

Signed _____

Name _____

Position _____

Date _____

For and on behalf of the Authority:

Signed _____

Name _____

Position _____

Date _____

SCHEDULE 3 – TENDER RESPONSE

Overview

Why Redhouse?

This is an exciting opportunity to use the CQC brand as it's meant to be used: as a powerful tool to achieve meaningful change. This is our heartland, and we have ideas to spare. We're the right agency for the job because we have:

1. the right approach
2. the right people
3. the right experience

The right approach

This piece of work will be fundamental to the organisation's success over the next five years. We'll take time up front to develop a strategic approach that is built on audience insights, is rigorously planned in a way that considers and engages all areas of the organisation, and is flexible enough to remain effective for the five-year lifespan of the project.

We know that a collaborative approach to this type of work will yield the best results. We'll invest time up front getting to know the complexities of your organisation, your team and your processes. We'll act as an extension of your team to combine our insights and creativity with your organisational knowledge.

For more about our approach, see page 11.

The right people

We'll give you an experienced senior team, dedicated to the account. This core senior team are all in-house employees who, together, have delivered four large brand engagement projects in the past year alone – you'll get the right blend of creative skills and implementation processes.

The team can call on in-house and trusted freelance resources when project workloads and timescales demand.

For more about our people, see page 6.

The right experience

As a brand agency, we're well used to helping aspirational brands define their story and build strategies to create the right connections with a diverse and complex stakeholder map. Our skills and experience fall into three areas:

- Brand definition – helping brands get to the heart of what they stand for
- Brand expression – bringing the story to life with a compelling visual and verbal language
- Brand engagement – implementing that language consistently across all internal and external touchpoints, campaigns, content strategy and creative design, to achieve targets and objectives.

We'll bring a rich heritage of healthcare communications, three decades' worth of experience delivering employee engagement and a real understanding of inspectorates and regulators to this assignment.

For more about our experience, see pages 6 - 16.

Accreditations

We are a rated supplier on the CIPS Sustainability Index and, as such, have been measured on the pillars: Financial, Environmental and Social. We are committed to conducting our business according to these rigorous ethical, professional and legal standards – and continuously improving our approach to these three areas.

We have CyberEssentials accreditation, which demonstrates our commitment to best practice in cyber-security

Leadership and experience

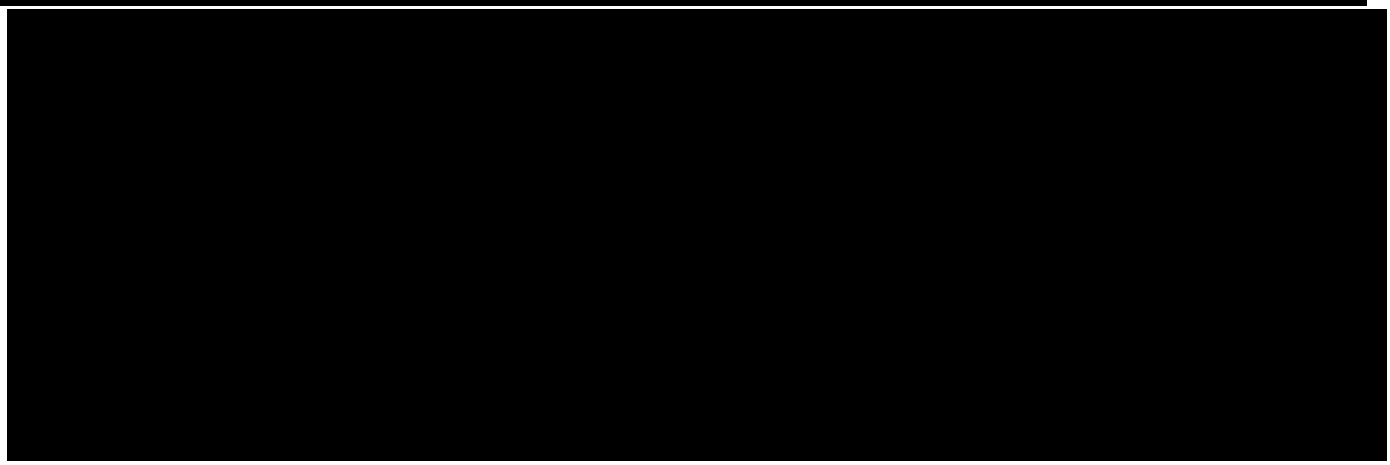
Our experience

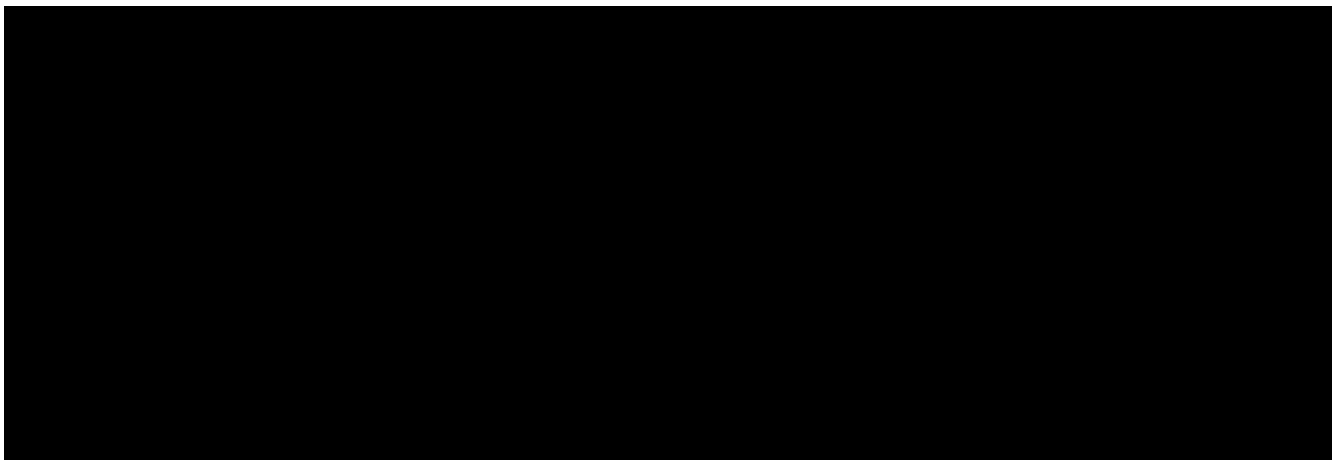
We have spent the past three decades working with government departments, health sector institutions and large corporates to deliver complex employee communications and transformation and change programmes.

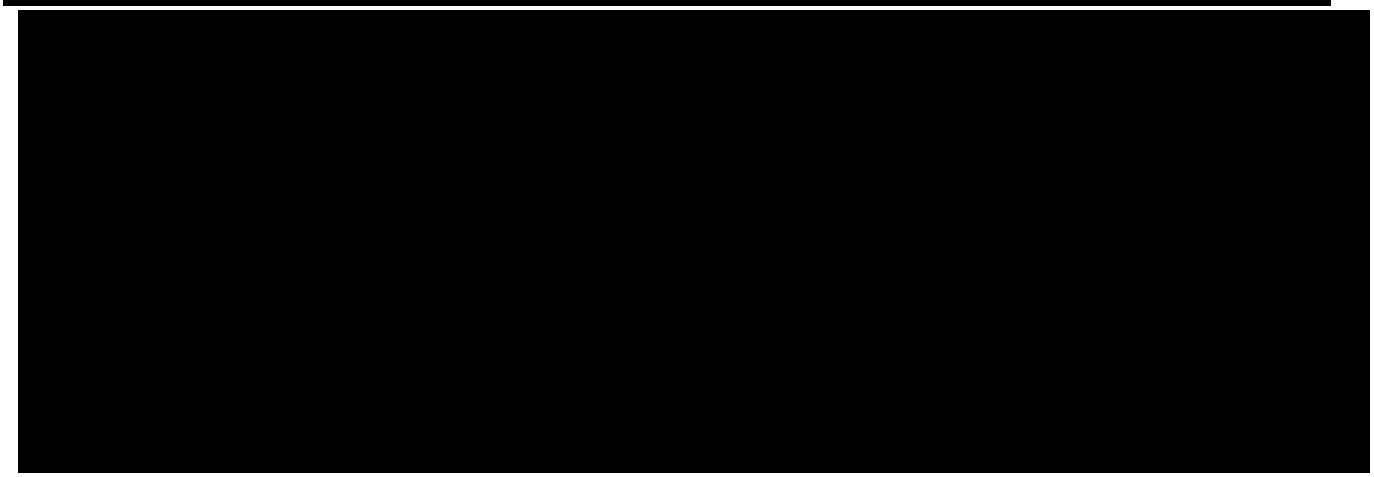
[redacted]

[redacted]

[redacted]







[redacted]

[redacted]

[redacted]

[redacted]

[redacted] ork [redacted] ~~museum installation Drone Aviary.~~

Methodology

Methodology: Bringing the ambition to life

We believe that effective employee communication and engagement will be fundamental to the success of your transformation programmes. To succeed we'll need to take a strategic and long-term approach, with a formal programme in which all elements are clearly defined.

We have developed a way of working that does this – based on the government's OASIS model.

- **Objectives:** what are the campaign's business objectives for each year until the transformation programmes are delivered?
- **Audience insight:** how does it segment; what are staff attitudes and behaviours? Your reference to work-silos and the high proportion of home-workers suggests this will be important for targeting, messaging and evaluation.
- **Strategy/Idea:** what messages and information do staff need to help deliver those objectives? How can we present this in an attention-grabbing way that will lead to behaviour change?
- **Implementation:** what channels and media are available? How should each best be used? When should messages be scheduled? What major events are forecast?
- **Scoring/Evaluation:** how can the impact and success of the campaign be measured?

Our first task will be to work with you to define, discuss and answer these questions – alongside practical considerations like budget and resourcing.

We will then summarise all these elements in a comprehensive strategy document, including our strategic intent, channel plan, a schedule for delivery and specific KPIs, designed to ensure buy-in from senior management.

These are some of the considerations that will underpin our initial discussions.

Co-create a new vision for the organisation

For people to buy into this transformation, we need to create a sense of ownership. We'll work with you to create a programme of work that starts by collaborating with team members from across the organisation, as well as senior management.

Our aim is to end up with a change narrative that people can point towards as 'theirs', and which is big, simple and true. By bringing people into things early, we'll create an opportunity to immediately help them understand why we're changing.

We'll design a series of staff workshops (and potentially other research techniques such as a survey) that gives us a strong platform of insights to build everything on.

A structured narrative

Five years is a long time for any organisation to maintain momentum and retain staff interest in any project. A common mistake is for organisations to feel they must communicate everything to everyone all at once.

We advocate a more drawn-out approach, where the basic principles are established – using our newly created vision to explain the 4-5 big picture messages that staff need to buy into – followed by a drip-feed of information and stories that reinforce them, targeted to the people that need them.

A compelling narrative

A compelling story is one that stands out, is understandable, relatable. In this instance it's also important to get people excited about the future. To do this, we will help you:

Create a coherent visual language

There are nine programmes within the transformation portfolio. We will bring these together within a single branded narrative. A unique visual language for the programme will ensure the programme resonates with your team.

Sell the benefits
Our mantra is "Focus on benefits". Every element of the programme, however small, should answer two questions:

- What's in it for our customers?
- What's in it for me?

Validate the benefits with examples from respected peer groups

A regular element of your narrative could be to show how other organisations have achieved similar transformations – and the benefits they have encountered. These organisations could include not only OGDs but aspirational brands such as Google and Apple.

Create the feeling of a shared journey
We need to dispel the notion that transformation is being imposed from above and show that this is a shared journey and purpose across the organisation by:

- Using members of staff to tell the story.
- Focusing on building shared experiences.

Focus on multi-channel and two-way storytelling

Top-down communication is rarely effective. Engagement is best achieved when the dialogue is happening up, down and across an organisation, with the shared learning and experiences that stem from them.

A realistic narrative

Experience suggests that many civil service staff are cynical about change. Some have "seen it all before". Others might see the new ways of working as just another way to save money. The way to win the resisters over is through:

- demonstrating success
- acknowledging issues, concerns and failures when they occur
- constantly recalibrating to show you're taking people's views seriously.

Demonstrate the new behaviours

Transformation will be a success once staff start to show the new behaviours required. The narrative should therefore provide practical illustrations of the behaviours.

Often the change is small scale. New technologies might offer all kinds of benefits, but it can prove difficult to achieve universal uptake.

So, alongside the big transformation messages, much of your communications might usefully centre around practical reinforcement and comprise a regular drip-feed of useful tips and hints.

Other clients we have helped establish a change narrative

- [redacted]

[redacted]

[redacted]

Resource Plan

We'd give you an experienced and dedicated team for the length of the contract.

This team would get to know CQC, understand the detail of the transformation programmes, gain insights into your audience and act as an extension of your in-house team.

- Client Partner (CP) – to oversee the project; establish KPIs; measurement protocols
- Change Engagement Specialist (CES) – to lead the engagement narrative development phase
- Head of Content (HC) – to develop narrative, messaging and copy platforms; creative content for campaigns
- Creative Director (CD) – to develop a visual identity for the programme; creative content for campaigns
- Designer (D) – creative content for campaigns
- Account Manager (AM) – day-to-day communication; scheduling; budgeting

It's hard to give you a firm Resource Plan without further discussion on methodology and priorities, but we'd envisage something like this to develop the engagement narrative:

Week 1	On-boarding meeting to set objectives; look at existing audience insights and research; agree methodology, research required, schedule and budget Background material to Redhouse	CP, CES, HC, CD, AM
Week 2	Desk research	CES, HC
Weeks 3-4	Individual meetings with senior leadership team, programme leads and comms team; employee groups (if appropriate)	CES, HC
Week 5-6	Research: workshop(s) and survey pulling together findings; developing audience personas; developing narrative; agreeing campaign plan	CES, HC, CP, CD
Week 8	Present strategy	CES, HC, CP
Week 9	Refine strategy	CES, HC
Week 10	Agree strategy, core messages and our creative brief	CES, HC, CD
Week 11-12	Creative concepting; draft copy platforms	CES, HC, CD
Week 14	Present campaign concept, look and feel and tone of voice	CES, HC, CD, CP
Week 15	Refine campaign concept, look and feel and copy platforms	CD, HC
Week 16	Agree concepts and copy	CD, HC, CP, AM
Week 18 onwards	Developing creative content and rollout	CD, Des, HC, CP, AM

Exit strategy and skills transfer

To ensure a smooth exit and skills transfer, we need to think about ways of working from the beginning.

This is about a close, collaborative ongoing relationship.

- If you can identify at an early stage the roles that will need the skills and knowledge at the end of the contract, we can ensure they are actively involved from the start.
- We'll share our creative rationales as we go along so the team really understands the concepts and how to apply them.
- We'd be happy to co-work and involve your team in 'roll-your-sleeves-up' brainstorming, strategy and planning sessions.
- We'll design our systems and processes to work when you take them on in-house (eg alignment of creative packages, file naming protocols, reporting).
- Your team are welcome to spend time working at our central London offices, and we're happy to come to you if that helps collaboration.
- We'll create a campaign toolkit with the background, copy, visual assets, etc, that you'll need to implement the programme consistently and successfully.
- We'll keep any measurement data we collate in an ordered way so you have access to it for benchmarking purposes.

Closer to the handover period, we'll agree a more formal handover with you. Staff may have changed and you may want us to re-visit some ways of working. This might include:

- Updated campaign concept toolkit
- Campaign guidelines
- Any research data gathered over the period
- A session where we hand over information and assets, share lessons learned and answer any questions
- A helpline/drop-in service for the first few months where we can advise on implementation, check adherence to the concept and answer questions.
- An end of phase one analysis report detailing what we learned, what went well and what can be improved in the next phase of work.

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

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

2. The contact details of the Processor's Data Protection Officer are: Jeremy Redhouse

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 and the Contractor is the Processor in accordance with Clause 13.1.
Subject matter of the processing	Staff feedback voluntarily provided on CQC Transformation plans from workshops/surveys/online comment.
Duration of the processing	One year maximum.
Nature and purposes of the processing	The data collected will only be for the purpose of providing themes from feedback to gauge views of groups. The data would be anonymised once feedback is collected and any personal data removed. Email personal data from projects would not be processed and only stored for the length of the contract. None of this data would be shared with third parties.

Type of personal data	Names and email addresses. Age, grade, job, location.
Categories of Data Subject	Staff
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	We would expect personal data to be destroyed within one month of feedback being themed after a survey. We would require that all personal data from projects to be destroyed by the contractor at the end of the contract.

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

SECURITY

All information about our clients is sensitive. 30 years' working on a variety of classified, politically sensitive and commercially sensitive projects for clients in Whitehall and the Private Sector brings with it an in-depth understanding and experience of security assessment and risk control. This has included working on some of the most high-profile and high-security projects for organisations such as the Cabinet Office, Ministry of Defence, The Security Service, Serious Organised Crime Agency, Cifas and the Atomic Weapons Establishment.

We consider the storing of client information, in a digital environment and indeed physically within our Clerkenwell studio, to be of the utmost importance. We have adapted our security measures appropriately to meet the needs of individual projects, for example:

- Secure paper disposal service
- Working off laptops supplied by clients and storing securely
- Clean desk policies
- Security clearance of personnel

Physical

- Current working files are housed on servers internal to Redhouse Lane.
- They are housed in our main office in a secured storage area, within sight of the manned reception desk.
- The hardware is fault tolerant with RAID5 data striping to ensure redundancy. Continuity
- Data is backed up nightly and stored on removable USB drives which are taken offsite nightly and stored securely by the Office Manager. This ensures that should something happen to the data onsite, we can restore from the previous day's work. Bi-annual full data backups are stored offsite in a fireproof safe.

Security

- File access is only granted to authenticated users on the network, with granting the least privileges necessary for the user to do their job.
- All data is secured via network authentication, i.e. you need a centrally created login to the systems that houses data.
- Active network scanning (AVG Business Security Suite) protects the data from virii, malware and cryptolocks. Updates are pushed out to endpoints automatically.
- Removable storage devices are discouraged within the company, unless necessary due to the size of the files we work with.
- Servers are physically secured to deter the insertion of external media and auto run is disabled.
- Remote access to data via SSL VPN is granted to some users. Access is only granted with the permission of Managing Director or Client Services Director.

Third Party

- Freelance workers do not have remote access to the data nor are they allowed to enter the company office without the attendance of a full time staff member.
- Their access to working files is managed by sharing via a separate file share segmented off the general file storage, they only get access to the specific collateral they need.
- Once a client job is finished, the entire job folder is moved to the archive NAS which is available to pertinent, authorised personnel only.
- If the client does not wish us to retain closed jobs and older data for archival purposes, we will delete and overwrite the disk space on which it was stored and comply with whichever mechanisms the client wishes us to use.
- Separate storage hardware can be provided if the client requires total isolation of data from Redhouse Lane's general working files, the cost to be provided upon application. This could be anything from external hard drive or an entire server dedicated to the clients files.
- Retired physical media is wiped via magnetisation to ensure total destruction of data and then disposed of responsibly.
- We can use public / private keys if the client wishes another layer of email security.
- Our email system allows us to remotely wipe the device should security be compromised.

Information Transfer

- Clients send us assets and information in a variety of ways – mostly via email, secure download, and hard copy on removable media or SDHC card.
- We have the ability to create isolated FTP sites for file transfer for clients or freelancers when necessary, ensuring that SFTP protocol is used.
- These logins are one time use and the FTP folder is decommissioned after use. Hard copies of assets are also sent via CD / DVD or portable hard drive – our anti-virus is configured to scan external media upon insertion. We make use of secure online transfer services such as YouSendIt.

Threat Protection and Management

- Digital information coming into Redhouse Lane, must pass through a firewalled intrusion detection system before entering our network.
- This unified threat management device logs activity, and send email alerts to IT personnel should anything suspicious be detected as well as alerting our ISP.
- Our network malware and anti-virus app continuously updates the endpoints, ensuring up to date threat management. It also controls the endpoint firewalls so that end-users cannot disable or change it.
- Internet access to clients and visitors to our offices is offered via a segmented Wi-Fi connection, without any path to our internal servers.
- Our company laptop uses an encrypted folder to store data within to secure it should the laptop be lost or stolen; it is also secured with local password and will be upgraded to two step authentication (SaasPass) by the end of the year (2016).
- We do not use removable or portable computing for sensitive client data - only for proposal and presentation work.
- Redhouse Lane has thus far not suffered an intrusion via our network from the internet side - over time there have been a number of attempts such as DOS attacks, etc. but as we have always had managed firewalling services, we have remained protected.
- In the event that we are hacked or we have an internal threat to the security of information we will respond by firstly nullifying the threat if possible, then proceed to investigate how it could have occurred and what the ramifications will be.

- We have not been externally security audited, but have so far relied on our internal scanning mechanism to alert us of any unusual network activity.

Certification

- We attained CyberEssentials Certification in November 2016. We have re-certified and our current certificate is valid until December 2019.

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 – NOT APPLICABLE

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?

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY

To be discussed at kick off meeting