

Contract (Short Form – Services)

Contract for the provision of Supporting innovation by GPs to reduce health inequalities in areas of deprivation, through better regulatory recognition and sharing of best practice

Contract Reference CQC PMS 001

September 2021

Contents

1	Interpretation.....	2
2	Priority of documents	12
3	Supply of Services	12
4	Term	13
5	Price, Payment and Recovery of Sums Due.....	14
6	Premises and equipment	15
7	Staff and Key Personnel	17
8	Assignment and sub-contracting.....	18
9	Intellectual Property Rights	19
10	Governance and Records.....	20
11	Confidentiality, Transparency and Publicity	21
12	Freedom of Information	23
13	Protection of Data	23
13A	Security
25		
14	Liability and Insurance	26
15	Force Majeure.....	27
16	Termination.....	28
17	Compliance.....	29
18	Prevention of Fraud, Corruption and Bribery	30
19	Dispute Resolution.....	32
20	General.....	32
21	Notices.....	34
22	Governing Law and Jurisdiction.....	35
23	TUPE	36

SCHEDULE 1 –SPECIFICATION.....**Error! Bookmark not defined.**

SCHEDULE 2 – PRICE39

SCHEDULE 3 – TENDER RESPONSE.....42

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS.....43

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN45

SCHEDULE 6 – CHANGE CONTROL74

SCHEDULE 7 – THIRD PARTY SOFTWARE – NOT USED.....76

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY77

THIS CONTRACT is dated 19th of Nov 2021

PARTIES

(1) **CARE QUALITY COMMISSION** of Citygate, Gallowgate, Newcastle Upon Tyne, NE1 4PA (“**Authority**”)

and

(2) Yorkshire and Humber Partners Academic Health Science Network Ltd (reg no. 08887451) whose registered address is **Unit 1, Calder Close, Calder Park, Wakefield, WF4 3BA** (“**Contractor**”)

(Together the “**Parties**”)

Background

1. The Authority is the independent health and social care regulator in England that monitors, inspects and regulates health and social care services to ensure they meet fundamental standards of quality and safety. It ensures health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve.
2. In order to Support innovation by GPs to reduce health inequalities in areas of deprivation, through better regulatory recognition and sharing of best practice.
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;

“Anti-Slavery and Human Trafficking Laws”	means all applicable anti-slavery and human trafficking laws, statutes, regulations, policies and codes from time to time in force including but not limited to the Modern Slavery Act 2015;
“Breach of Security	means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor system, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract;
“Central Government Body”	<p>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:</p> <ul style="list-style-type: none">(a) Government Department;(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);(c) Non-Ministerial Department; or(d) Executive Agency;
“Change Control Notice (“CCN”)”	means a change control notice in the form set out in Schedule 6;
“Contract”	means the contract consisting of these terms and conditions, any attached Schedules, the invitation to tender including Specification, the Tender Response and Award Letter between the Authority the Contractor;

“Contract Period”	shall mean the Term of the Contract;
“Confidential Information”	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
“Contractor”	means the person named as Contractor who was awarded this contract;
“Contractor’s Response”	means the document submitted by the Contractor to the Authority in response to the Authority’s invitation to suppliers for formal offers to supply the Services appended hereto in Schedule 3;
“Contractor System”	means the information and communications technology system used by the Contractor in performing the Services including the Software, the Contractor Equipment and related cabling (but excluding the Authority System);
“Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer”	shall each have the same meaning given in the GDPR;
“Data	means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii)

Protection Legislation	the DPA 2018 [subject to Royal Assent] to the extent that it relates to the processing of Personal Data and privacy; (iii) all applicable Law about the processing of Personal Data and privacy;
“Data Loss Event”	means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
“Data Subject Request”	means a request made by or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access his or her Personal Data;
“DPA”	means the Data Protection Act 2018 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such legislation;
“Default”	means any breach of the obligations of the relevant Party (including abandonment of the Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of the Contract and in respect of which such Party is liable to the other;
“Expiry Date”	means the date for expiry of the Contract as set out in the Award Letter;

“FOIA”	means the Freedom of Information Act 2000;
“GDPR”	means the General Data Protection Regulation (<i>Regulation (EU) 2016/679</i> ;
“Good Industry Practice”	means standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances;
“Grant Funding Agreement”	The agreement entered into between the Authority and the Secretary of State for Business Energy and Industrial Strategy to contribute to certain expenditure in undertaking supporting innovation by GPs to reduce health inequalities in areas of deprivation, through better regulatory recognition and sharing of best practice;
“Information”	has the meaning given under section 84 of the FOIA;
“Joint Controllers”	means where two or more Controllers jointly determine the purposes and means of processing;
“Key Personnel”	means any persons specified as such in the Specification or Contract otherwise notified as such by the Authority to the Contractor in writing;
“Law”	means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply;
“LED”	means Law Enforcement Directive (<i>Directive (EU) 2016/680</i>)

“Loss”	means any losses, costs, price, expenses, interest, fees (including legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, price, fines, damages, destruction, adverse judgments, orders or other sanctions and the term “ Losses ” shall be construed accordingly;
“Party”	means the Contractor or the Authority (as appropriate) and “Parties” shall mean both of them;
“Premises”	means the location where the Services are to be supplied, as set out in the Specification;
“Price”	means the price (excluding any applicable VAT) payable to the Contractor by the Authority under the Contract, as set out in Schedule 3 for the full and proper performance by the Contractor of its obligations under the Contract;
“Pricing Schedule”	means Schedule 3 containing details of the Price;
“Processing”	has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted accordingly;
“Processor Personnel”	means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract;
“Prohibited Act”	means: <ul style="list-style-type: none"> (a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: <ul style="list-style-type: none"> i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity;

(b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with the Contract;

(c) an offence:

- i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act;
- ii) under legislation or common law concerning fraudulent acts; or
- iii) the defrauding, attempting to defraud or conspiring to defraud the Authority;

any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct has been carried out in the UK;

“Protective Measures”	means appropriate technical and organisational measures which include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule 5 (Security Requirements and Plan);
“Purchase Order 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;
“Relevant Requirements”	means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for

Justice pursuant to section 9 of the Bribery Act 2010;

“Replacement Contractor”	means any third party supplier appointed by the Authority to supply any services which are substantially similar to any of the Services in substitution for any of the Services following the expiry, termination or partial termination of the Contract;
“Request for Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Schedule”	means a schedule attached to, and forming part of, the Contract;
“Security Plan”	means the Contractor’s security plan prepared pursuant to paragraph 3 of Schedule 5 (Security Requirements and Plan), an outline of which is set out in an Appendix to Schedule 5;
“Security Policy Framework”	means the HMG Security Policy Framework (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf)
“Services”	means the services to be supplied by the Contractor to the Authority under the Contract as set out in Schedule 1;
“Specification”	means the specification for the Services (including as to quantity,

description and quality) as specified in Schedule 1;

“Staff” means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor engaged in the performance of the Contractor’s obligations under the Contract;

“Staff Vetting Procedures” means vetting procedures that accord with good industry practice or, where requested by the Authority, the Authority’s procedures for the vetting of personnel as provided to the Contractor from time to time;

“Sub-Contractor” means a third party directly or indirectly contracted to the Contractor (irrespective of whether such person is an agent or company within the same group of companies as the Contractor) whose services are used by the Contractor (either directly or indirectly) in connection with the provision of the Services, and “**Sub-Contract**” shall be construed accordingly;

“Sub-processor” means any third Party appointed to process Personal Data on behalf of the Processor related to this Contract;

“Supplier Code of” means the HM Government Contractor Code of Conduct dated September 2017;

Conduct”

- “Term” means the period from the start date of the Contract set out in the Award Letter to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Contract;
- “Third Party Software” means software which is proprietary to any third party which is or will be used by the Contractor to provide the Services including the software and which is specified as such in Schedule 7;
- “TUPE” means the Transfer of Undertakings (Protection of Employment) Regulations 2006;
- “VAT” means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
- “Variation” means a variation to the Specification, the Price or any of the terms and conditions of the Contract;
- “Working Day” means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

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

- 1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;
- 1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

- 1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Contract;
- 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
- 1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Priority of documents

- 2.1 In the event of, and only to the extent of, any conflict between the clauses of the Contract, any document referred to in those clauses and the Schedules, the conflict shall be resolved in accordance with the following order of precedence:
 - a) these terms and conditions
 - b) the Schedules
 - c) any other document referred to in these terms and conditions

3 Supply of Services

- 3.1 In consideration of the Authority's agreement to pay the Price, the Contractor shall supply the Services to the Authority for the Term subject to and in accordance with the terms and conditions of the Contract.
- 3.2 In supplying the Services, the Contractor shall:
 - 3.2.1 co-operate with the Authority in all matters relating to the Services and comply with all the Authority's instructions;
 - 3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Contractor's industry, profession or trade;

- 3.2.3 use Staff who are suitably skilled, experienced and possess the required qualifications to perform tasks assigned to them, and in sufficient number to ensure that the Contractor's obligations are fulfilled in accordance with the Contract;
- 3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;
- 3.2.5 comply with all applicable laws; and
- 3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.
- 3.3 The Authority may by written notice to the Contractor at any time request a Variation to the scope of the Services. If the Contractor agrees to any Variation to the scope of the Services, the Price shall be subject to fair and reasonable adjustment to be agreed in writing between the Authority and the Contractor.
- 3.4 Any Variation will not take effect unless recorded in a Change Control Notice in the form set out in Schedule 6 and approved in writing by the Authority.
- 3.5 In the event that this Contract or any Purchase Order terminates or expires, the Contractor shall, if requested to do so by the Authority, continue to provide the Services commenced prior to the date of such termination or expiry at no extra cost to the Authority other than the continued payment of the Price for such Services. The Contractor shall comply with its obligations in accordance with the Exit Management Strategy in Schedule 8.

4 Term

- 4.1 The Contract shall take effect on 07/09/2021 and shall expire on the Expiry Date, 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 6 months subject to further funding by giving not less than 10 Working Days' notice in writing to the Contractor prior to the Expiry Date. The terms and conditions of the Contract shall apply throughout any such extended period.

5 Price, Payment and Recovery of Sums Due

- 5.1 The Price for the Services shall be as set out in Schedule 2 and shall be the full and exclusive remuneration of the Contractor in respect of the supply of the Services. Unless otherwise agreed in writing by the Authority, the Price shall include every cost and expense of the Contractor directly or indirectly incurred in connection with the performance of the Services.
- 5.2 The Contractor shall invoice the Authority as specified in Schedule 2. Each invoice shall include such supporting information required by the Authority to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.
- 5.3 In consideration of the supply of the Services by the Contractor, the Authority shall pay the Contractor the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number. The Authority may, without prejudice to any other rights and remedies under the Contract, withhold or reduce payments in the event of unsatisfactory performance.
- 5.4 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Authority shall, following the receipt of a valid VAT invoice, pay to the Contractor a sum equal to the VAT chargeable in respect of the Services.
- 5.5 If there is a dispute between the Parties as to the amount invoiced, the Authority shall pay the undisputed amount. The Contractor shall not suspend the supply of the Services unless the Contractor is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.
- 5.6 If a payment of an undisputed amount is not made by the Authority by the due date, then the Authority shall pay the Contractor interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.
- 5.7 If any sum of money is recoverable from or payable by the Contractor under the Contract (including any sum which the Contractor is liable to pay to the Authority in respect of any breach of the Contract), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Contractor under the Contract or under any other agreement or contract with the Authority. The Contractor shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

- 5.8 Where the Contractor enters into a sub-contract, the Contractor shall include in that sub-contract:
- 5.8.1 Provisions having the same effect as clauses 5.2 to 5.6 of the Contract and
 - 5.8.2 Provisions requiring the counterparty to that subcontract to include in any sub-contract which it awards provisions having the same effect as clauses 5.2 to 5.6 of this Contract.
 - 5.8.3 In this clause 5.8 'sub-contract' means a contract between two or more Contractors, at any stage of remoteness from the Authority in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract.

6 Premises and equipment

- 6.1 If necessary, the Authority shall provide the Contractor with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Authority's premises by the Contractor or the Staff shall be at the Contractor's risk.
- 6.2 If the Contractor supplies all or any of the Services at or from the Authority's premises, on completion of the Services or termination or expiry of the Contract (whichever is the earlier) the Contractor shall vacate the Authority's premises, remove the Contractor's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Authority's premises in a clean, safe and tidy condition. The Contractor shall be solely responsible for making good any damage to the Authority's premises or any objects contained on the Authority's premises which is caused by the Contractor or any Staff, other than fair wear and tear.
- 6.3 If the Contractor supplies all or any of the Services at or from its premises or the premises of a third party, the Authority may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.
- 6.4 The Authority shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Authority's premises the Contractor shall, and shall procure that all Staff shall, comply with all the Authority's security requirements.

- 6.5 Where all or any of the Services are supplied from the Contractor's premises, the Contractor shall, at its own cost, comply with all security requirements specified by the Authority in writing.
- 6.6 Without prejudice to clause 3.2.6, any equipment provided by the Authority for the purposes of the Contract shall remain the property of the Authority and shall be used by the Contractor and the Staff only for the purpose of carrying out the Contract. Such equipment shall be returned promptly to the Authority on expiry or termination of the Contract.
- 6.7 The Contractor shall reimburse the Authority for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Contractor or any Staff. Equipment supplied by the Authority shall be deemed to be in a good condition when received by the Contractor or relevant Staff unless the Authority is notified otherwise in writing within 5 Working Days.
- 6.8 Any Premises/land made available from time to time to the Contractor by the Authority in connection with the contract, shall be made available to the contractor on a non-exclusive licence basis free of charge and shall be used by the contractor solely for the purpose of performing its obligations under the contract. The Contractor shall have the use of such Premises/land as licensee and shall vacate the same on completion, termination or abandonment of the Contract.
- 6.9 The Parties agree that there is no intention on the part of the Authority to create a tenancy of any nature whatsoever in favour of the Contractor or its Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Authority retains the right at any time to use any premises owned or occupied by it in any manner it sees fit.
- 6.10 Should the Contractor require modifications to the Premises, such modifications shall be subject to prior Approval and shall be carried out by the Authority at the Contractor's expense. The Authority shall undertake approved modification work without undue delay. Ownership of such modifications shall rest with the Authority.
- 6.11 All the Contractor's equipment shall remain at the sole risk and responsibility of the Contractor, except that the Authority shall be liable for loss of or damage to any of the Contractor's property located on Authority's Premises which is due to the negligent act or omission of the Authority.

7 Staff and Key Personnel

- 7.1 If the Authority reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Contract, it may, by giving written notice to the Contractor:
- 7.1.1 refuse admission to the relevant person(s) to the Authority's premises;
 - 7.1.2 direct the Contractor to end the involvement in the provision of the Services of the relevant person(s); and/or
 - 7.1.3 require that the Contractor replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Authority to the person removed is surrendered,
- and the Contractor shall comply with any such notice.
- 7.2 The Contractor shall:
- 7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures; and if requested, comply with the Authority's Staff Vetting Procedures as supplied from time to time;
 - 7.2.2 if requested, provide the Authority with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Authority's premises in connection with the Contract;
 - 7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Authority; and
 - 7.2.4 shall at all times comply with the Supplier Code of Conduct (<https://www.gov.uk/government/publications/Contractor-code-of-conduct>).
 - 7.2.5 ensure that it does not engage in any act or omission that would contravene Anti-Slavery and Human Trafficking Laws.
- 7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Authority, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.

- 7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Authority (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.
- 7.5 At the Authority's written request, the Contractor shall provide a list of names and addresses of all persons who may require admission in connection with the Contract to the Premises, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Authority may reasonably request.
- 7.6 The Contractor's Staff, engaged within the boundaries of the Premises shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when at or outside the Premises.
- 7.7 The Authority may require the Contractor to ensure that any person employed in the provision of the Services has undertaken a Criminal Records Bureau check as per the Staff Vetting Procedures.

8 Assignment and sub-contracting

- 8.1 The Contractor shall not without the written consent of the Authority assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Contract or any part of the Contract. The Authority may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Contractor shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.
- 8.2 If the Contractor enters into a Sub-Contract for the purpose of performing its obligations under the Contract, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Contractor to the Sub-Contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.
- 8.3 If the Authority has consented to the placing of Sub-Contracts, the Contractor shall:
 - (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 provide short monthly reports on the delivery of the Services and would include updates on the progress made, risks and mitigation plans and next steps
 - 10.1.2 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 provide information about their Services progress, the aims and objectives as well as the lessons learnt and expected long-term benefits.
 - 10.1.3 produce a final report outlining achievements, lessons learned from the performance of the Services and next steps (if relevant).
- 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.
- 11.5 The Contractor must seek prior approval from the Authority within a reasonable time prior to publicising, carrying out promotional activities or disseminating information concerning the Services.
- 11.6 The Authority must ensure that any publicity material for the Services is compliant with the publicity terms of the Grant Funding Agreement.

12 Freedom of Information

- 12.1 The Contractor acknowledges that the Authority is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall and procure that any sub-contractor shall:
 - 12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;
 - 12.1.2 transfer to the Authority all Requests for Information relating to this Contract that it receives as soon as practicable and in any event within 2 Working Days of receipt;
 - 12.1.3 provide the Authority with a copy of all Information belonging to the Authority requested in the Request for Information which is in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may reasonably specify) of the Authority's request for such Information; and
 - 12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Authority.
- 12.2 The Contractor acknowledges that the Authority may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Contractor or the Services (including commercially sensitive information) without consulting or obtaining consent from the Contractor. In these circumstances the Authority shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Contractor advance notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.
- 12.3 Notwithstanding any other provision in the Contract, the Authority shall be responsible for determining in its absolute discretion whether any Information relating to the Contractor or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

13 Protection of Data

13.1 Authority Data

- 13.1.1 The Contractor shall not delete or remove any proprietary notices contained within or relating to the Authority Data.
- 13.1.2 The Contractor shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Contractor of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.
- 13.1.3 To the extent that Authority Data is held and/or Processed by the Contractor, the Contractor shall supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification.
- 13.1.4 The Contractor shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data.
- 13.1.5 The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored securely off-site. The Contractor shall ensure that such back-ups are made available to the Authority immediately upon request.
- 13.1.6 The Contractor shall ensure that any system on which the Contractor holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework.
- 13.1.7 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Contractor's Default so as to be unusable, the Authority may:
 - (a) require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data and the Contractor shall do so promptly; and/or
 - (b) itself restore or procure the restoration of Authority Data, and shall be repaid by the Contractor any reasonable expenses incurred in doing so.
- 13.1.8 If at any time the Contractor suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Contractor shall notify the Authority immediately and inform the Authority of the remedial action the Contractor proposes to take.

13.2 **Personal Data**

13.2.1 The Parties agree that on commencement of the contract, there will be no personal data to be processed in the provision of the Services under this Contract. However, should there be any changes during the Term of the Contract and personal data is shared and processed during the provision of the Services, other than information that is already in the public domain, Schedule 4 (Processing, Personal Data and Data Subjects) will be varied to include the relevant provisions on data protection.

13.2.2 Subject to clause 13.2.1, the Parties acknowledge that for the purposes of the Data Protection Legislation, the Parties are independent Controllers in their own right.

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

13A Security

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

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

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

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

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

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

14 Liability and Insurance

- 14.1 The Contractor shall not be responsible for any injury, loss, damage, cost or expense suffered by the Authority if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under the Contract.
- 14.2 Subject always to clauses 14.3, 14.4 and 14.5:
- 14.2.1 the aggregate liability of the Contractor in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Contract, the supply or failure to supply of the Services, misrepresentation (whether tortious or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the Price payable to the Contractor under this Contract [whichever is higher]; and
- 14.2.2 except in the case of claims arising under clauses 9.4 and 18.4 in no event shall the Contractor be liable to the Authority for any:
- a) loss of profits;
 - b) loss of business;
 - c) loss of revenue;
 - d) loss of or damage to goodwill;
 - e) loss of savings (whether anticipated or otherwise); and/or
 - f) any indirect, special or consequential loss or damage.
- 14.3 Nothing in the Contract shall be construed to limit or exclude either Party's liability for:
- 14.3.1 death or personal injury caused by its negligence or that of its Staff;
- 14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or

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

14.4 The Contractor's liability under the indemnity in clauses 9.4 and 18.4 shall be unlimited.

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

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

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

15 Force Majeure

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

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

16 Termination

- 16.1 The Authority may terminate the Contract at any time by notice in writing to the Contractor to take effect on any date falling at least 1 month (or, if the Contract is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.
- 16.2 Without prejudice to any other right or remedy it might have, the Authority may terminate the Contract by written notice to the Contractor with immediate effect if the Contractor:
- 16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Contract which is not capable of remedy;
 - 16.2.2 repeatedly breaches any of the terms and conditions of the Contract in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Contract;
 - 16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Contractor receiving notice specifying the breach and requiring it to be remedied;
 - 16.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;
 - 16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13, 17, 18.4 and 20.11; or
 - 16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Contractor (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Contractor's assets or business, or if the Contractor makes any

composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction.

- 16.3 The Contractor shall notify the Authority as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.
- 16.4 The Contractor may terminate the Contract by written notice to the Authority if the Authority has not paid any undisputed amounts within 90 days of them falling due.
- 16.5 If the Authority terminates the Contract under this clause, the Authority shall make no further payments to the Contractor except for Services supplied by the Contractor prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority.
- 16.6 Termination or expiry of the Contract shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 13A, 14, 16.7, 17.4, 18.4, 19 and 20.8 or any other provision of the Contract that either expressly or by implication has effect after termination.
- 16.7 Upon termination or expiry of the Contract, the Contractor shall:
 - 16.7.1 give all reasonable assistance to the Authority and any incoming Contractor of the Services to the extent necessary to effect an orderly assumption by a Replacement Contractor in accordance with the procedure set out in Schedule 8 – Exit Management Strategy; and
 - 16.7.2 return all requested documents, information and data to the Authority as soon as reasonably practicable.

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:

Citygate, Gallowgate, Newcastle Upon Tyne, NE1 4PA

For the attention of: [REDACTED]

[REDACTED]

21.3.2 For the Contractor:

Yorkshire and Humber Partners Academic Health Science Network Ltd

Unit 1, Calder Close, Calder Park, Wakefield, WF4 3BA

For the attention of: [REDACTED]

[REDACTED]

[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.

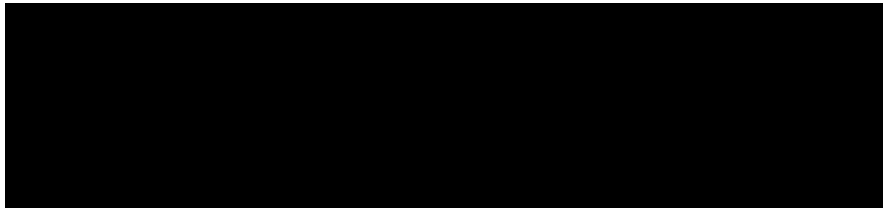
22 Governing Law and Jurisdiction

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.

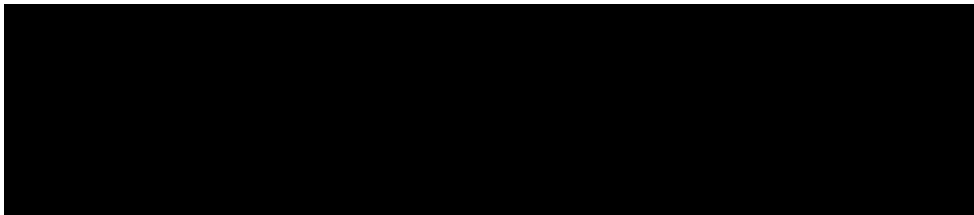
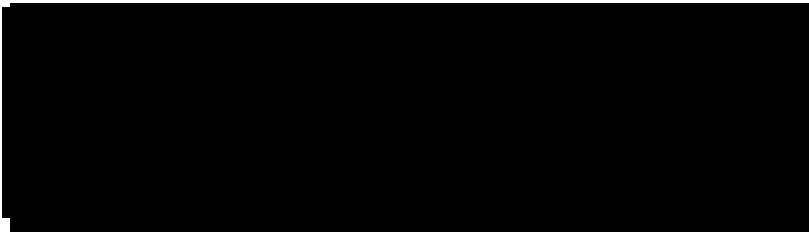
23 TUPE – NOT USED

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**

A large black rectangular redaction box covering the signature and name of the Care Quality Commission representative.

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

A large black rectangular redaction box covering the signature and name of the Contractor representative.A black rectangular redaction box covering the signature and name of the Contractor representative.



SCHEDULE 1 –SPECIFICATION

Introduction

Evidencing innovative practice has been difficult for many GP practices, particularly those situated in socio-economically deprived areas. In addition to this, it is often difficult to evidence any innovative practice to address health inequalities in Care Quality Commission (CQC) regulatory processes unless the project has a direct effect on achieving a healthcare target. We have heard that this inability to have innovative practice acknowledged can have significant effects on the rating of a GP practice making it less likely for them to be able to achieve 'good' or 'outstanding' rating. Consequently, despite these efforts, struggling and already under-resourced GP practices may remain in a cycle of inequality and are unable to recruit and retain staff and may also encounter difficulties with funding.

Our project aims to develop a toolkit which can guide GP practices through developing innovative projects to reduce health inequalities which can then be evidenced in the CQC regulatory process. We also wish to review the CQC methodology so that GP's find it easier to have their work acknowledged and used in ratings. Lastly, we wish to be able to share learning from various projects so that other may implement similar strategies amongst their own populations to improve health inequalities nationwide.

We hope that the project would primarily be a gain for GP practices due the likelihood of improved regulatory outcomes. There may also be an impact on future funding of their work if they are able to successfully evidence the impact and outcomes of their innovative projects.

The project will directly provide dedicated support measures on innovation around health inequalities and may therefore enable major improvements in health outcomes. This will be achieved by providing an appropriate regulatory environment which recognised innovation in health inequalities and assists hard-pressed GP practices to showcase and share innovation.

We are working collaboratively with the Yorkshire and Humber Academic Health Science Network (Y&H AHSN) to understand the challenges GPs face in innovation and develop a toolkit which can ameliorate this problem. Y&H AHSN have extensive expertise in both innovation and health inequalities. Their Chief Executive plays a leading role on health inequalities for the AHSN Network nationally and is working with NHS England to define the role innovation can play in tackling inequalities. They have undertaken a

number of projects supporting innovation in primary care and have excellent reach into the networks of GP practices we will need to access to deliver the project. We have worked together to plan the project, building on our respective expertise.

Y&H AHSN have set out a budget for their element of the work of £55,782 (inclusive of VAT at standard rate) funded by Regulators' Pioneer Fund. It will run from September 2021 – March 2022.

The Contractor shall:

- Develop materials/ a “tool” to help GP practices provide evidence of innovation to reduce health inequalities, working with us, volunteer GP practices and other experts in the field
- Work with some volunteer GP practices to test the tool and get feedback – from us and from them
- Produce a final version of the tool
- Supply us some case study examples to use
- Clearly inform practices to be engaged in the study how the information they provide will be used, shared and published.

Expectations from the Contractor

- Establish team working relationships with team within CQC
- Produce a review of the relevant literature for the CQC to use in the project, including the final report
- Set up and conduct fieldwork including structured interviews and roundtable discussion groups, and undertake case studies with relevant practices
- Attend working group meetings with CQC
- Publicise the project to GP practices in order to recruit practices to be involved in the work
- Liaise with CQC to develop a joint engagement plan to keep practices regularly informed as the project progresses
- Produce a fieldwork report detailing findings from structured interviews, roundtable discussion groups, and case studies
- Share fieldwork report and recommendations with CQC colleagues and stakeholders as appropriate
- Work with volunteer GP practices to develop and test a final ‘tool kit’ and/or materials to help practices to evidence innovation
- Produce a report of the methodology used in developing the toolkit
- Develop outline action plan for implementation
- Work with CQC to deliver a final report
- Attend and provide input to working group meeting

- Collaboratively draw up an Information Sharing Agreement to govern confidential personal information to be shared.

SCHEDULE 2 – PRICE

Project financial information

[illegible]

Payment terms

30 days after invoice date

SCHEDULE 3 – CONTRACTOR’S RESPONSE

There was no bidding process. Award of the contract progressed based on Single tender arrangement with Y&H AHSN for the following reasons:

- T [REDACTED] has a leading role on health inequalities on behalf of the AHSN Network nationally, and is working with NHS England's Health inequalities team to define the role that innovation can play in this agenda.
- They have a lot of experience in innovation in primary care, for example Healthy Hearts [Reducing heart attacks and strokes in West Yorkshire - YHAHSN](#). The initiative aims to improve care by making better use of existing primary care resources and maximising clinical engagement. Since the beginning of the project: Nearly 17,500 patients have their hypertension better controlled to safe limits below 140/90. Because of this, over the next 5 years, an estimated 350 people will avoid a heart attack or stroke. Other examples include working with primary care to develop and evaluate innovative services which are enabled using healthy.io (smartphone-based urinalysis) and Tytocare (remote examination). [Guest blog: Smartphone self-care for people with diabetes - YHAHSN](#), [Pilot programmes launched to transform health care at home - YHAHSN](#)
- This means they also already have excellent reach into networks of GP practices which we will need to reach quickly to deliver the work
- They have an agile way of working, so can bring resources to deliver on stream quickly – necessary for a very short term project. If we had to tender for this work, we would be unlikely to be able to deliver in the timescale required to accept the funding bid.
- Y&H as a region has a mix of types of areas of deprivation – from inner city areas to coastal towns

To summarise, they are the ideal partner in terms of their national engagement on the issues that we are working on and their local ability to deliver high quality work in a short timescale.

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

Please refer to clause 13.2

Data Processing Schedule

1. The contact details of the Controller's Data Protection Officer are: Nimali de Silva, Care Quality Commission, Citygate, Gallowgate, Newcastle upon Tyne NE1 4PA.
2. The contact details of the Processor's Data Protection Officer are: Clair Long, Population, email: clair.long@yhahsn.com
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	<p>The Parties are independent Controllers in their own right in accordance with clause 13.2.1.</p> <p>Please refer to clause 13.2</p>
Subject matter of the processing	N/A on commencement of the Contract.
Duration of the processing	N/A on commencement of the Contract.
Nature and purposes of the processing	N/A on commencement of the Contract.
Type of personal data	N/A on commencement of the Contract.
Categories of Data Subject	N/A on commencement of the Contract.
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	N/A on commencement 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



YORKSHIRE & HUMBER
ACADEMIC HEALTH SCIENCE NETWORK

Data Protection Policy

Reference: POL04
Version: 1.0
Effective date: 12/11/2019
Classification: Internal
Owner: CEO

Internal Use Only

Printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY.

Data Protection Policy

Version History

Version	Date	Author	Summary of changes
0.1	24/01/2019		NEW – draft
0.2	13/03/2019		Amended draft, updated job titles & section 4.5 to reference Breathe HR
0.3	25/09/2019		Amended draft following final review by Head of Strategic Projects.
1.0	12/11/2019		Amended wording in section 4.2

Data Protection Policy

Contents

Version History.....	2
1. Purpose	4
2. Scope.....	4
3. Applicable standards and requirements	4
4. Policy statement.....	4
4.1. Introduction and definitions	5
4.2. Data Protection Principles.....	6
4.3. Dealing with subject access requests and other disclosures.....	8
4.4. Providing information over the phone	9
4.5. Retention and Disposal of Data	9
4.6. Publication of information.....	10
4.7. Direct Marketing	10
4.8. Privacy by Design and Data Protection Impact Assessments (DPIAs)	10
4.9. Breaches	11
4.10. Complaints	11
4.11. Penalties	11
4.12. Compliance and monitoring	11
5. Supporting documents	11
6. Approval.....	12

Data Protection Policy

1. Purpose

The purpose of this policy is to ensure that Yorkshire & Humber Academic Health Service Network (YHAHSN) conduct their business practices in a manner compliant with the UK Data Protection Act (DPA) 2018 and EU General Data Protection Regulations (GDPR) 2016 and its principles to ensure that all personal data is secure, accurate and up-to-date at all times. For the purpose of this policy, all references to GDPR also includes the Data Protection Act 2018.

2. Scope

This policy and the guidance (which is set out in the following pages) applies to all staff (including managers), consultants and any third party that this policy has been communicated to, as it is the responsibility of all to assist us in complying with our obligations as data controller. All members of staff should familiarise themselves with both this policy and the guidance and apply their provisions in relation to any processing of personal data. Failure to comply with the GDPR, the Policy and the Guidance could amount to misconduct, which is a disciplinary matter, and could ultimately lead to summary dismissal. Serious breaches could also result in personal criminal liability.

For these reasons, it is important that all employees familiarise themselves with this Policy and the Guidance and attend any training sessions in respect of the care and handling of Personal Data.

3. Applicable standards and requirements

Standard	Applicable requirement
GDPR and DPA	Article 24
ISO27001:2013	A.18.1.4 Privacy and protection of personally identifiable information

4. Policy statement

("YHAHSN, we, us, our"), as Data Controller, is committed to ensuring its compliance with the requirements of the law governing the management and storage of Personal Data (as defined below), which is set out in the UK's Data Protection Act 2018 and the EU's General Data Protection Regulation 2018 ("GDPR"). We recognise the importance of Personal Data to our business and the importance of respecting the privacy rights of individuals. This Data Protection Policy ("the Policy") sets out the principles which we will apply to our Processing (as defined below) of Personal Data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with applicable laws.

Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office ("ICO"). YHAHSN is accountable to the ICO for its data protection compliance.

This policy aims to protect and promote the data protection rights of individuals and of the business, by informing everyone working for the business of their data protection obligations and of the business procedures that must be followed in order to ensure compliance with GDPR. Information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This policy covers all personal data and special categories of personal data, however processed (on computers or manually). In the event that any staff process personal data through working at home, for example, this Guidance and all it entails applies equally to such data.

This policy and the guidance may be amended from time to time to reflect any changes in practice or legislation. The Data Protection Officer is responsible for monitoring the business's compliance with this policy and any queries as to data protection procedures or requirements should be directed to the Corporate Services Manager (designated Data Protection Officer).

This policy has been approved by the CEO. It will be reviewed every two year or as and when a change in the data protection regime requires it to be updated.

Data Protection Policy

4.1. Introduction and definitions

YHAHSN, as data controller, is required to comply with the GDPR in respect of its processing of personal data (such as information about our customers, employees and suppliers). Compliance with data protection legislation is the responsibility of all members of the business who process personal information and it is therefore important for all staff to familiarise themselves with both the data protection policy and this guidance and act in accordance with their content.

Any day-to-day data protection issues or any questions about the policy or the guidance should be raised with the Data Protection Officer.

The GDPR is intended to protect the rights and privacy of individuals and to ensure that data about them is not processed without their knowledge and the legal basis for processing must be established to ensure it is fair, lawful and transparent. Whilst the GDPR covers Personal Data relating to individuals, you should bear in mind that if you handle personal details of, for example, officers of companies, this will still constitute personal data and therefore be subject to the GDPR's requirements.

It should be noted that the business is authorised to process data connected to staff administration, advertising and marketing and keeping accounts and records. Anyone who is/ intends-processing data for purposes not included in the business's entitlements should seek advice from the Data Protection Officer.

In this Guidance, the following definitions are used:

Consent is agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, have given their agreement to the processing of personal data relating to them.

Data controllers means the natural or legal person, public authority, agency or other body who alone or jointly with others, determine the purposes for which, and the manner in which, any Personal Data is processed. They have a responsibility to establish practices and policies in line with the GDPR. YHAHSN is the data controller of all personal data used in our business.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Data subjects (for the purpose of this policy) include all living, identified or identifiable individuals about whom YHAHSN holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data. This will include, and is not limited to, staff, customers, suppliers and business contacts.

Personal data means data (however held) relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address, date of birth or telephone number) or it can be an opinion (such as a performance appraisal). It will include passport or driving licence details. It also includes information that identifies the physical, physiological, genetic, mental, economic, cultural or social identity of a person. For the business's purposes, our customers are data subjects (other individual third parties that we hold personal data about are also likely to be data subjects)

Processing is any activity that involves use of the personal data. It includes obtaining, recording or holding the data, or carrying out any operation on or regarding the data including organising, accessing, amending, merging, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or making available personal data to third parties.

Special categories of personal data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special categories of personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Protection Policy

4.2. Data Protection Principles

- All Data Subjects have rights with regard to how their personal data is handled. During our activities we will store and process personal data which includes information about our staff and our customers and suppliers. We recognise the requirement to treat this information correctly and in a lawful manner.
- Personal data, which may be held on paper or on a computer, is subject to certain legal safeguards specified in the GDPR and other regulations. The GDPR imposes restrictions on how we may use that information.
- YHAHSN has to adhere to the data processing principles around which the GDPR is based. These principles deal with handling, processing, transportation, destruction and storage of personal data. It is essential that all staff adhere to these principles in performing their day-to-day duties. The principles require the business to ensure that all personal data and special categories of personal data:
 1. is processed fairly and lawfully and in a transparent manner in relation to the subject;
 2. shall be obtained for specified, explicit and legitimate purposes and not processed in a way that is incompatible with these purposes;
 3. shall be adequate, relevant and not excessive in relation to the purpose it is held;
 4. shall be accurate and kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay;
 5. shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed;
 6. shall be processed in accordance with the individuals' rights; and
 7. shall be processed in a manner that ensures appropriate technical and organisational measures shall be taken against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

Additionally, personal data shall not be transferred to a country or territory outside the European Economic Area unless: (1) that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data; (2) appropriate, approved standard contractual clauses are in place; (3) the Data Subject has given explicit consent; or (4) the transfer is necessary for a reason set out in the GDPR. If this is envisaged, speak to the Data Protection Officer for further guidance before transferring any data.

The business must be able to demonstrate its compliance with the above principles ('accountability').

In order to process all personal data in a manner that is compliant with GDPR, we will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet our obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held can be fully exercised under applicable laws;
- take the appropriate technical and organisational security measures to safeguard personal data; and
- ensure that personal data is not transferred abroad without suitable safeguards.

To expand on the practical aspects of the principles:

Fair and lawful Processing

Lawfulness, Fairness and Transparency

The GDPR is intended not to prevent the processing of personal data, but to ensure that it is done lawfully, fairly and in a transparent manner in relation to the individual and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, certain conditions have to be met, and YHAHSN will aim to process personal data in line with contractual obligations, legal obligations or legitimate business interests, if this is not possible we may ask the data subject to consent to the processing, that it is in connection with us delivering our services for the data subject supported by a privacy notice at a minimum.

When special categories of personal data is being processed, more than one condition must be met. In most cases, the data subject's explicit consent to the processing of such data will be required.

Data Protection Policy

Evidence of consent and records of all consents should be kept so that the business can demonstrate compliance with consent requirements.

Processing for specific and limited purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose and consent obtained before any processing occurs.

Adequate, relevant and non-excessive Processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place. If you are in possession of excessive data, it should be immediately deleted or destroyed. We must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the business's data retention guidelines.

Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate and therefore you should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out of date data should be destroyed or updated as appropriate. You should notify the HR Manager with regard to any of your own personal data which needs updating and you should also ensure that if any customer or third party provides updated personal information, the update is acted upon without delay.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose, meaning that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is to be kept before being destroyed, contact the Data Protection Officer.

Processing in line with Data Subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- ask what information YHASN holds about them and why;
- request access to any personal data held about them by us;
- prevent the processing of their data for direct marketing purposes;
- ask to have inaccurate data amended;
- prevent processing that is likely to cause damage or distress to themselves or anyone else;

if we have any, be informed of the mechanics of any automated decision-making process that will significantly affect them;

- not have significant decisions that will affect them taken solely on an automated process;
- sue for compensation if they suffer damage as a consequence of a contravention of data protection laws; and
- request the Information Commissioner (the regulatory authority on this subject) to assess whether any provision of applicable laws has been contravened.

Data Security

- To guard against the risk of unlawful or unauthorised processing of personal data, or against the accidental loss of, or damage to, personal data, we will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own and identified risks. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.
- The GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if that third party agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. As an example, you may wish to consider password protecting emails or documents being transmitted to third party recipients or if the email or document contains particularly delicate or special categories of personal data, confirming by telephone (i.e. separately) to the intended recipient what the password is. We use Office 365 which includes email encryption technology for this purpose. Ask IT for training if required.
- Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data. These are defined as follows:
 - **Confidentiality** means that only people who are authorised to use the data can access it. All

Data Protection Policy

- staff are responsible for ensuring that any Personal data which they hold is kept securely and that it is not disclosed to an unauthorised third party;
- **Integrity** means that Personal data should be accurate and suitable for the purpose for which it is processed;
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our hosted systems instead of on individual PCs.
- Security procedures include:
 - **Passwords.** Computer passwords must be kept confidential.
 - **Entry controls.** Any unannounced stranger seen in entry-controlled areas or beyond "normal" visitor access areas should be politely challenged as to their purpose and their presence should be queried with the Data Protection Officer.
 - **Secure lockable desks and cupboards.** Such should be kept locked if they hold confidential information of any kind. Note that personal data is always considered confidential.
 - **Methods of disposal.** Paper documents containing personal data, once no longer needed, should be placed in the shredding bins. Hard drives or any permitted memory sticks should be specifically erased before disposal and floppy disks and CD-ROMs should be physically destroyed when no longer required.
 - **Equipment.** Staff should ensure that individual monitors do not show confidential information to passers-by or to any person to whom this policy does not apply and that they lock or log off from their PC when it is left unattended. Any portable devices should be encrypted when not in use and never left unattended.
 - **Memory Sticks.** For data security purposes, writing to memory sticks has been prohibited without prior approval. If you need to save information to a memory stick, speak to the Corporate Service Manager for provision of a memory stick.

The GDPR requires us to keep full and accurate records of all our data processing activities. We must keep and maintain accurate records reflecting our Processing including records of data subjects' consents and procedures for obtaining consents. These records should include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the Personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

If you have any concerns about processing personal data, please contact the Data Protection Officer who will be happy to discuss matters with you.

4.3. Dealing with subject access requests and other disclosures

The GDPR gives rights to individuals in respect of the personal data organisations hold about them. Everyone must be familiar with these rights and adhere to the business's procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of personal data;
- Right to make a complaint to the regulatory authority, the Information Commissioner's Office.

A formal request from a Data Subject for information that we hold about them need not be in any particular format but it should specify the information that the data subject requires. If you receive a request for personal data and require guidance as to whether it is a "subject access request", speak to the Data Protection Officer. We will require the data subject to provide evidence of their identity (so we are not disclosing to a third party). Any member of staff who receives a written request should forward it to the Data Protection Officer immediately who will assist. A request sent by email or fax is as valid as one sent in hard copy. Requests may also be validly made by means of social media. Note that information requested under a subject access request may not be fully disclosable as particular exemptions from disclosure may apply. Indeed, it may be that none of the information is disclosable. The Data Protection Officer will advise as to what can be disclosed.

Data Protection Policy

YHAHSN aims to comply with requests for access to personal information as quickly as possible, and, if we hold such information, will ensure that it is provided within one month of the request unless there is a proper reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

We must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and, in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data on an individual to a third party. Speak to the Data Protection Officer if in doubt.

Personal data may be legitimately disclosed where one of the following conditions applies:

- The individual has given their consent (e.g. consenting to us speaking to their adviser or other named third party);
- Where disclosure is in the legitimate interests of the business (e.g. disclosure to other staff members);
- Where the business is legally required to disclose the data.

The GDPR contains some exemptions in respect of disclosures. If you are contacted by:

- the Police;
- any government department asking for information about customers;

you must not confirm or deny whether or not we hold information about a data subject. If you receive a Production Order from the Police or an order from a government department requiring information to be disclosed, contact the Data Protection Officer.

4.4. Providing information over the phone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal or confidential information held by us. In particular they should:

- check the caller's identity to make sure that information is only given to a person who is entitled to it;
- suggest that the caller put their request in writing if they are not sure about the caller's identity or the purpose of the enquiry and where their identity cannot be checked;
- refer to the Data Protection Officer for assistance in difficult situations. No-one should be pressured into disclosing personal information.

Every member of staff that holds information about identifiable living individuals must comply with the GDPR in managing that information.

4.5. Retention and Disposal of Data

The business will not retain Personal Data for longer than necessary.

- **Customers:** Data for customers is generally retained where relevant for a customer's lifespan for the legitimate purposes of our business or otherwise for seven years once no longer a customer, in order to comply with legal and regulatory requirements.
- **Staff:** We use an HR company, Breathe HR, to create a personnel file for each member of staff and will keep this for the duration of employment and for a minimum of six months after a staff member leaves employment. After six months, we will review the personnel file and delete any personal data that we do not need. We will retain the following personal data for the following periods of time:

Data	Period of Retention
Data confirming payments due to you. For example, your contract of employment and any information about salary or benefits.	6 years after you leave your employment

Data Protection Policy

Data relating to taxes, National Insurance contributions and other charges paid in relation to you.	7 years after you leave your employment
Data relating to any accidents or injuries at work.	3 years after you leave your employment
Data relating to any references given in relation to you.	1 year after the date of the reference

- **Recruitment Records:** Breathe HR will also deal with all recruitment records, including unsuccessful candidates.
- **Disposal of Records:** all Personal Data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g. shredding).

4.6. Publication of information

The business publishes a number of items that includes personal data and will continue to do so. These include:

- Internal telephone directory
- Staff information/photographs on the firm's website
- Information including photographs in newsletters, tender applications and so on.

4.7. Direct Marketing

Before any electronic direct marketing is undertaken, it must be clear that the people to be contacted have consented to receive such marketing and that a valid, up to date, consent notice is held on file. There is a limited exception for existing customers known as "soft opt in" – this allows us to send marketing texts or emails if we have obtained contact details in the course of providing services to that person, the messages are marketing similar services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

For marketing by post, we are able to send postal marketing to our customers regarding new products or services, in reliance on our "legitimate interests" – we generally do not need consent to this type of mailing but we will always need to offer customers an opt-out.

The right to object to direct marketing must be explicitly offered to the data subject. A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

4.8. Privacy by Design and Data Protection Impact Assessments (DPIAs)

Privacy by Design involves using appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles. Privacy by design is an ongoing measure.

Data Privacy Impact Assessments (DPIA) involve using tools and assessments to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

DPIAs will be carried out when introducing, or making significant changes to, systems or projects involving the Processing of Personal Data. DPIAs are required to identify data protection risks and to assess the impact of these risks, as well as to determine appropriate action to prevent or mitigate the impact of these risks.

This means thinking about whether we are likely to breach the GDPR and what the consequences might be, if we use Personal Data in a particular way. It is also about deciding whether there is anything that we can do to stop or minimise the chances of potential problems identified, from happening.

Data Protection Policy

4.9. Breaches

A data protection breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Everybody working for us has a duty to report any actual or suspected data protection breach without delay to the Data Protection Officer or, in their absence, their line manager.

Breaches will be reported to the ICO by the Data Protection Officer without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, unless, we are able to demonstrate that the Personal Data breach is unlikely to result in a risk to the rights and freedom of Data Subjects. Where there is a high risk to the rights and freedoms of individuals, we must also notify the affected individuals.

The Data Protection Officer will maintain a central register of the details of any data protection breaches.

4.10. Complaints

Complaints relating to breaches of the GDPR and/or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to the Data Protection Officer without delay.

4.11. Penalties

It is important that everyone understands the implications for the business if we fail to meet our data protection obligations. Failure to comply could result in:

- Criminal and civil action
- Personal accountability and liability
- Suspension/withdrawal of the right to process personal data by the ICO which would impact on our ability to do business
- Loss of confidence in the integrity of our systems and procedures
- Irreparable damage to our reputation

Breaches can have serious consequences. YHAHSN could be fined up to 20,000,000 Euros, or up to 4% of annual turnover of the preceding financial year, whichever is the higher and depending on the breach.

4.12. Compliance and monitoring

Activities relating to data protection will be monitored, and failure to comply could lead to disciplinary action which may result in termination of employment/contract.

5. Supporting documents

Document reference and title
POL02 Information Security Policy
POL07 Data Retention Policy
PRD02 Data Subject Access Request Procedure
PRD03 Data Protection Impact Assessment Procedure
PRD07 Complaints Procedure

Data Protection Policy

6. Approval

Approved by: Richard Stubbs
Job Title: CEO
Date: 12/11/2019

END OF DOCUMENT



YORKSHIRE & HUMBER
ACADEMIC HEALTH SCIENCE NETWORK

Health and Safety Policy

Reference: POL20
Version: 1.0
Effective date: 14/04/2021
Classification: Internal
Owner: Director of Corporate Services

Internal Use Only

Printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY.

Health and Safety Policy

Version History

Version	Date	Author	Summary of changes
0.1	01/04/2021	Sarah Dykes	NEW – draft
1.0	27/04/2021	Sally Hawkworth	Approved

Health and Safety Policy

Contents

Version History.....	2
1. Purpose	4
2. Scope.....	4
3. Applicable standards and requirements	4
4. Policy statement.....	5
4.1. Objectives.....	8
4.2. Responsibilities	8
5. Supporting documents	8
6. Approval.....	8

Health and Safety Policy

1. Purpose

The implementation and maintenance of health and safety policies and procedures is vital to the success of Yorkshire and Humber Academic Health Science Network (YHAHSN).

To manage the risks to an acceptable level by the design, implementation and maintenance of a health and safety management policy.

To comply with applicable legal and regulatory requirements.

2. Scope

All Yorkshire & Humberside Academic Health Science Network (YHAHSN) personnel and suppliers, employed under contract

3. Applicable standards and requirements

Standard	Applicable requirement
Health and Safety at work act 1974	To comply with
Environmental Protection Act 1990	To comply with
Management of Health and Safety at Work Regulations 1999	To comply with

Health and Safety Policy

4. Policy statement

YHAHSN is committed to:

Complying with the Health & Safety at Work Act 1974 and Management of Health and Safety at Work Regulations 1999 as well as other health, and safety legislation.

Protecting and Safeguarding the health, safety and welfare of our employees, contractors, visitors and public from risks arising from our work activities.

Providing and Maintaining a safe place of work and safe work equipment for our employees.

Providing sufficient resources to achieve our aims and objectives.

Promoting a positive **Safety Culture** in which all employees, contractors and visitors share.

Managing our activities so as to prevent accidents, near-misses and work-related ill health hazards.

Monitoring, Auditing and Reviewing our safety performance and revising our Health and Safety Management Systems to ensure that we achieve our objective of continuous improvement.

Co-operating with our clients to maintain high safety standards.

Managing Health and Safety matters as a critical business activity and integral part of our commitment to excel

4.1. Environmental Policy Statement

The Company recognises that to have a planned approach to the prevention and reduction of waste and pollution leads to a long term reduction of costs.

The Company will control its activities to avoid unnecessary and unacceptable risks or adverse effects on the environment, in line with the requirements of the Health and Safety at Work Act 1974 and the Environmental Protection Act 1990.

Environmental awareness and individual responsibility will be developed amongst employees at all levels and effective consultation will be encouraged. The Company will develop and improve standards by making use of available technology and developments, together with waste recovery and a recycle approach.

Clients, employees and the general public who may be affected will be made aware of any Company activity that may affect the environment.

Environmental action

Management will take individual responsibility to ensure that environmental issues are considered when making decisions and when planning or controlling works.

Workforce

All employees must recognise their individual responsibilities for carrying out their works in a sympathetic manner with respect to the environment.

Waste reduction

All employees must give careful consideration to the elimination and reduction of waste at every stage.

Where recycling or re-use of material is an economical advantage this will be considered.

This Policy will be reviewed annually.

Health and Safety Policy

4.2. Responsibilities for Health and Safety

4.2.1 Directors

The above has overall responsibility for ensuring that the Health and Safety Policy is put into practice. In particular to ensure that:

- Employees receive sufficient information, training and supervision on health and safety matters
- A risk assessment is undertaken and the results recorded and made available to all employees
- Accidents are investigated and reviewed
- Safe and healthy work conditions are provided and maintained
- Each employee is aware of his/her individual responsibilities
- Sound and safe working practices are understood and observed
- Appropriate safety equipment and protective clothing for the task is provided and worn correctly.

4.2.2 Employees

All employees are responsible for ensuring that they:

- Have read and understood the risk assessments
- Comply with the requirements of the risk assessments and work in a safe manner at all times
- Wear protective clothing and use safety equipment at all times as appropriate
- Report defects in equipment or materials immediately to management
- Maintain tools and equipment in good condition
- Use equipment for the purpose which it was intended
- Only use the equipment upon which they have been trained
- Report to management all accidents, dangerous occurrences and near misses
- Do not interfere with or misuse anything provided to ensure their safety
- Accidents are reported to management

4.3. Risk Assessment

The health and safety risks arising from our work activities will be assessed using the process of risk assessment in accordance with The Management of Health and Safety at Work Regulations 1999.

The responsibility for ensuring that risk assessments have been undertaken and recorded and appropriate action is taken to control risks is that of the Corporate Services Manager.

The written risk assessments will be reviewed and updated annually to ensure that they cover all employees against all risks and to ensure that any actions identified in the risk assessments have been implemented. The risk assessments will also be updated every time that there are any major changes in work practices.

4.4. Fire

There is a fire alarm on site and this is tested weekly.

Fire extinguishers are provided and are inspected on an annual basis.

Smoking is not allowed on site.

IN THE EVENT OF FIRE

1. An individual discovering a fire must alert other members of staff and people working in the area by activating the nearest available break glass point.
2. If it is completely safe to do so a member of staff should attack the scene of the fire using the nearest extinguisher.
3. On hearing the fire alarm all staff must evacuate the building using the nearest available fire escape, making other staff aware they must leave the premises.

Health and Safety Policy

4. If safe to do so all windows and doors should be closed behind them, electrical items should be switched off if time permits and if safe to do so.
5. Once outside the premises all staff should report to their designated meeting point in the car park.

Fire Wardens are responsible for undertaking the head count , including obtaining the visitors book if it is safe to do so and reporting the results of this to the Fire Service.
6. No-one should re-enter the premises once evacuated.
7. Once all employees and visitors are accounted for they must remain in the designated meeting point unless stated by the Fire Service.

4.5. Electrical Safety

Yorkshire & Humber Academic Health Science Network has a duty of care under the Electricity at Work Regulations 1989 to ensure that the risk from electricity is reduced to the lowest level.

Compliance with these Regulations is the responsibility of the Director.

All fixed plant and installations must be routinely inspected and tested in accordance with current legislation and best practice.

The fixed electrical installation is inspected every 5 years.

Portable appliances are tested on a regular basis.

All electrical work is carried out by third parties who have been assessed as competent for the task being carried out.

4.6. Accident Procedure/First Aid

All accidents are recorded in the virtual accident book, this is in the Corporate Services section of the YHSHAN Intranet. Completed forms are then sent to the Corporate Services Manager for confidential filing.

Major accidents i.e. those involving a major injury or more than 7 days off work will be fully investigated using the following form. Accidents required to be reported under RIDDOR will be reported by the Corporate Services Director.

RIDDOR reportable accidents are outlined below:

Reportable specified injuries are:

- Fracture, other than to fingers, thumbs and toes.
- Amputation of arm, hand, finger, thumb, leg, foot or toe.
- Loss of sight (temporary or permanent).
- Any crush injury to head/torso causing damage to brain or internal organs.
- Any burn injury resulting in burns of 10% of whole body or significant damage to eyes, respiratory system or other vital organs.
- Any degree of scalping requiring hospital treatment.
- Any loss of consciousness caused by head injury or asphyxia.
- Any other injury arising from work in a confined space leading to hypothermia, heat-induced illness or unconsciousness; or requiring resuscitation; or requiring admittance to hospital for more than 24 hours.

In addition, any accident that occurs at work and that involves more than 7 days off work are also required to be reported.

The current list of reportable dangerous occurrences is available on the HSE website.

Health and Safety Policy

First aid boxes are located in each kitchen and in the fire marshall cupboard.

The current first aiders are:

Angela Foster

Sally Creese

Christine Johns

4.7. Objectives

The objectives of YHAHSN's Health and Safety procedures are renewed annually inline with Health and Safety consultant Sarah Dykes of Sarah Dykes Ltd.

4.8. Responsibilities

- The Director of Corporate Services will create and review this policy.
- Senior Leadership Team facilitates the implementation of this policy through the appropriate standards and procedures.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective areas.
- All personnel and contracted suppliers follow the procedures to maintain the information security policy.
- All personnel have a responsibility for reporting security incidents and any identified weaknesses.
- Any deliberate act to jeopardise the health and safety of any staff member, contractor or visitor to YHAHSN or their customer or suppliers will be subject to disciplinary and/or legal action as appropriate.

5. Supporting documents

Document reference and title
DOC13 Accident Form
DOC37 H&S Risk Assessment Form
DOC67 Home Working Checklist
DOC69 DSE Questionnaire
DOC60 Fire Evacuation Employee Checklist

6. Approval

Approved by:

Job Title:

Date:



END OF DOCUMENT

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.

SCHEDULE 6 – CHANGE CONTROL

Contract Change Note

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

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

IT IS AGREED as follows

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

Change Requestor / Originator		
Summary of Change		
Reason for Change		
Revised Contract Price	Original Contract Value	£
	Previous Contract Changes	£
	DN: Enter all CCN's here so that total value is shown for Audit purposes	
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details)		
DN: Any change to Specification should be added as an Annex to the CCN		
Revised 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 [INSERT DATE] or from the date on which both the Authority and the Contractor have communicated acceptance of its terms.

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

SCHEDULE 7 – THIRD PARTY SOFTWARE – NOT USED

CONTRACTOR SOFTWARE

For the purposes of this Schedule 7, “**Contractor Software**” means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services. The Contractor Software comprises the following items:

Software	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