Information Handling/Security policy

Approved by	PF and G P Governors & Mr I Brown Link Governor
Date Approved	25.05.2018
Version	1
Review Date	Annually

SCHEDULE 1

Information Handling

1. Definitions and Interpretation

1.1 In this Schedule 1 the following terms shall have the meaning set out below:

"Authority Data"

means any 'information' provided by, obtained or created on behalf of Nottinghamshire County Council in delivering the services specified in this contract; and in the case of Personal Data, any data processed on behalf of the Authority where it is the Data Controller.

"Caldicott Principles (1997, 2012 & 2016)"

means the Caldicott principles which protect patient identifiable data. These principles are applicable to any processing of health or social care data.

"Data Protection Act 1998 (DPA)"

means the Data Protection Act 1998 (DPA) being replaced by GDPR on 25th May 2018

"Data Protection Officer"

means the role as defined under Chapter IV, Section 4 of GDPR

"Environmental Information Regulations 2004 (EIR)"

means the Environmental Information Regulations 2004 (EIR) as amended or re-enacted from time to time and any Act substantially replacing the same.

"Freedom of Information Act 2000 (FOIA)"

means the Freedom of Information Act 2000 (FOIA) as amended or re-enacted from time to time and any Act substantially replacing the same.

"Good Industry Practice"

means the exercise of the degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced contractor engaged in the same type of undertaking under the same or similar circumstances as are contemplated by this Agreement;

“General Data Protection Regulation (GDPR)”

means the General Data Protection Regulation (2016), Regulation (EU) 2016/679, as amended or re-enacted from time to time and any United Kingdom Act or European Union Regulation recognised in UK law substantially replacing the same. All compliance references to GDPR in this Agreement are applicable from 25th May 2018

“Information”

has the meaning given under Section 84 of the Freedom of Information Act 2000 (FOIA), which shall include (but is not limited to) information in any form whether relating to the past, present or future and may in particular consist of data, documentation, programs, (including the source code of any programs which the Authority has the right to use), computer output, voice transmissions, correspondence, calculations, plans, reports, graphs, charts, statistics, records, projections, maps, drawings, vouchers, receipts and accounting records and may consist of or be stored in any form including paper, microfilm, microfiche, photographic negative, computer software and any electronic medium and references herein to Information shall include reference to the medium in which it is stored.

“Information Legislation”

means the DPA, FOIA, GDPR and the EIR.

“Information Policy Requirements”

means the documented set of additional information governance requirements which the Authority applies within itself and requires of its Contractors and of which it has furnished a copy to the Contractor via a link to the Authority’s website

“Legislation”

for the avoidance of doubt includes all Law in particular the Information Legislation.

“Personal Data”

means personal data as defined in Section 1 (1) of the DPA and Article 4 (2) of the GDPR, which is supplied to the Contractor by the Authority or obtained by the Contractor in the course of performing the Services.

“Subject Access Request”

means a request for Personal Data falling within the provisions of Section 7 of the DPA and Article 15 of the GDPR

2. Resolution of Inconsistency

2.1 The Contractor shall immediately upon becoming aware of the same notify the Authority of any inconsistency between its practices and the provisions of Information Legislation, including related regulation, standards, guidance and policies applicable under this Schedule and compliance statements made by the Contractor during the contract procurement process

2.2 Where notified or it otherwise becomes aware of inconsistency the Authority, as soon as practicable, shall advise the Contractor which provision the Contractor shall be required to comply with (but not so as to place the Contractor in breach of any Legislation) by means of an Action Plan which:

2.2.1 specifies the inconsistency and articulates the resulting risks posed to the Authority's compliance with legislation

2.2.2 explains how the requirement to resolve the inconsistency meets the contractual requirements and the statements of compliance made during the tender process

2.2.3 specifies the time period which in the Authority's opinion is reasonable in which to resolve the inconsistency

2.2.4 explains the means by which the Authority intends to satisfy itself that the inconsistency is resolved and specifies the steps the Contractor is required to take to facilitate any assessment

2.2.5 takes into account the opinion of the Contractor on the level of resource required to resolve the inconsistency

2.3 Where inconsistencies are not resolved within the expectations set out in paragraph 2.2, the Authority may use the dispute resolution provisions of this contract

3. Protection of Information

3.1 The Contractor acknowledges that the confidentiality, integrity and availability of Information and on the security provided in relation to Information is a material element of this Agreement.

3.2 The Contractor shall and shall at all times provide a level of security which:

3.2.1 is in accordance with Legislation and this Contract

3.2.2 is in accordance with compliance regimes representing Good Industry Practice which the Authority may specify

3.2.3 complies with the Information Policy Requirements; and

3.2.3 meets any specific security threats identified from time to time by the Authority

3.3 The Contractor shall ensure that it provides comparable technical and policy coverage of security to Information as if it were being processed directly by the Authority. This shall include but not limited to the following:

3.3.1 All mobile storage systems and hardware shall be encrypted to at least industry standards.

3.3.2 All employees shall be appropriately vetted before use in the services which are the subject of this Agreement.

3.3.3 All employees shall receive adequate information governance training which shall be annually refreshed.

3.3.4 All buildings and physical environments shall be subject to appropriate physical security and protection.

3.3.5 When handling NHS data, the Contractor shall apply Safe Haven usage to at least NHS standard and comply with the requirements of the Caldicott Principles.

3.3.6 The Contractor shall permit access to Information by employees of the Authority only as may be specifically designated by the Authority.

3.3.7 The Contractor shall securely destroy all Information provided or created under this Agreement and no longer required to be retained in accordance with this Agreement.

3.4 The Contractor will have in place fully tested and effective disaster recovery and business continuity plans.

3.5 The Contractor shall observe the following principles when handling personal data for the purpose of carrying out the Contractor's obligations under this Agreement.

3.5.1 Every proposed processing of Personal Data within or outside the contractor's organisation should be clearly defined and regularly risk assessed and approved by an appropriate information governance role holder.

3.5.2. Personal Data must not be processed unless it is absolutely necessary. Personal Data should not be used unless there is no alternative.

3.5.3 The minimum necessary Personal Data is to be used. Where use of Personal Data is considered necessary, each individual item of information should be justified with the aim of reducing the need for processing personally identifiable information.

3.5.4 Access to Personal Data should be on a strict need to know basis. Employees should only have access to the data that they need to see, and should only receive the access and functionality permissions required to undertake their roles

3.5.5 The Contractor must ensure that its employees are aware of their responsibility to comply with the common law duty of confidentiality.

3.5.6 All persons handling Personal Data must understand and comply with the DPA. All processing of Personal Data must be lawful.

3.6 Any Information received by the Contractor from the Authority under this Agreement or generated by the Contractor pursuant to this Agreement shall remain at all times the property of the Authority. It shall be identified, clearly marked and recorded as such by the Contractor on all media and in all documentation.

3.7 The Contractor shall not, save as required by this Agreement, without the prior written consent of the Authority disclose to any other person any Information provided by the Authority under this Agreement.

3.8 The Contractor shall advise the Authority of any intention to procure the services of any other agent or subcontractor in connection with this Agreement and shall pay due regard to any representations by the Authority in response, or obtain the express consent of the Authority for arrangements where Personal Data may be processed.

3.9 The Contractor shall observe and comply with the Authority's security classification/ protective marking scheme as defined within its Information Policy Requirements

3.10 The Contractor shall take all necessary precautions to ensure that all Information obtained from the Authority under or in connection with this Agreement, is given only to such of the Contractor's employees and professional advisors or consultants engaged to advise the Contractor in connection with this Agreement as is strictly necessary for the performance of this Agreement, and is treated as confidential and not disclosed (without prior written approval) or used by any such employees or such professional advisors or consultants otherwise than for the purposes of this Agreement.

3.11 The Contractor shall not use any Information it receives from the Authority otherwise than for the purposes of this Agreement.

3.12 With regard to Authority Data:

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

3.12.2 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 Agreement or as otherwise expressly authorised in writing by the Authority.

3.12.3. To the extent that Authority Data is held and/or processed by the Contractor, the Contractor shall supply that Authority Data to the Authority as requested by the Authority in the format specified in the Information Assets Register as set out in Schedule 2 (Goods and/or Services Specification).

3.12.4. The Contractor shall take responsibility for preserving the integrity of Authority Data and preventing the corruption or loss of Authority Data

3.12.5 The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Business Continuity and Disaster Recovery Plan. The Contractor shall ensure that such back-ups are available to the Authority at all times upon request and are delivered to the Authority at no less than monthly intervals.

3.12.6 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 Authority's Information Policy Requirements

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

3.12.7.1 require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data in full and in not later than three Days (subject to any agreed business continuity and disaster recovery plan); and/or

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

3.12.8 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.

4. Data Protection

4.1 The Authority is and will remain the Data Controller in relation to the personal information processed under this Agreement, and that the Contractor will act as Data Processor with respect to such personal information. As such, the Contractor must follow the direction of the Authority as to how Personal Data is processed.

4.2 All Personal Data acquired by the Contractor from the Authority shall only be used for the purposes of this Agreement and shall not be further processed or disclosed without the prior written consent of the Authority.

4.3 The Contractor shall comply with the GDPR requirements with regard to appointing a Data Protection Officer

4.4 The Contractor warrants that it has given appropriate notification under the DPA under registration number [number] to undertake the subject matter of this Agreement.

4.5 The Contractor shall comply with all relevant codes of practice issued under the DPA (and GDPR when in force)

4.6 The Contractor shall assist the Authority in safeguarding the legal rights of the data subject

4.7 The Contractor will have in place at all times appropriate technical and organisational security measures to safeguard Authority Data in compliance with DPA and National Cyber Security Centre (NSNC) guidance.

4.8 The Contractor shall indemnify the Authority against loss, destruction or processing contrary to the DPA by itself, its employees, contractors or agents.

4.9 The Contractor shall ensure the reliability and training of all its relevant employees to ensure awareness of and compliance with the Contractor's obligations under the DPA.

4.10 The Authority shall respond to all Subject Access Requests (SAR), whether received by the Contractor or the Authority, and therefore the Contractor shall provide to the Authority the personal data requested by the Data Subject (as defined in the DPA) within 10 working days of receipt of instruction by the Authority for supply of the data.

4.11 The Contractor shall immediately notify a senior manager within the Authority if it receives:

4.9.1 a request from any person whose Personal Data it holds to access his Personal Data; or

4.9.2 a complaint or request relating to the Authority's obligations under the DPA

4.12 The Contractor will assist and co-operate with the Authority in relation to any complaint or request received, including:

4.10.1 providing full details of the complaint or request;

4.10.2 providing the Authority with any information relating to a SAR within 10 working days of receipt of the request;

4.10.3 promptly providing the Service Manager with any Personal Data and other information requested by him.

4.13 In addition to the obligation undertaken in paragraph 4.4.8, the Contractor shall not further process information outside of the EEA as defined by the DPA without full prior written consent from the Authority.

4.14 The Contractor shall cooperate with Data Protection Compliance Audits as and when requested.

4.15 The Contractor shall comply with GDPR requirements for maintaining accurate, current and comprehensive Records of Processing

5. Caldicott Principles

5.1. The Contractor must also observe the Caldicott Principles when processing health and/or social care data, which are set out below.

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don’t use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each discrete item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical employees — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

6. The FOIA and the EIR

6.1 The Authority is subject to the provisions of the FOIA and the EIR and the Contractor shall assist the Authority (at the Contractor's expense) to enable the Authority to comply with these Acts. The Contractor acknowledges that the Authority may be obliged to disclose Information relating to this Agreement. Notwithstanding any other term of this Agreement, the Contractor hereby gives its consent for the Authority to publish this Agreement in its entirety, including from time to time agreed changes to the Agreement, to the general public in whatever form the Authority decides.

6.2 The Contractor must transfer any request for information under FOIA and EIR to the Authority as soon as practicable after receipt and in any event within 2 working days of receipt.

6.3 Where the Authority so requires for the purpose of compliance with the Information Legislation, the Contractor shall provide the Authority with a copy of all Information in its possession or power, in the form that the Authority requires, within 10 working days (or such other reasonable period as the Authority may specify) of the Authority requesting the Information

6.4 Without prejudice to paragraph 5.6 and subject to paragraph 5.8 below, where the Contractor believes the disclosure of information would prejudice its commercial interests or constitute an actionable breach of confidentiality, the Authority shall consider any case made where it is provided within 10 working days (or such other reasonable period as the Authority may specify) of the Authority requesting the Information

6.5 The Contractor shall provide all necessary assistance as requested by the Authority under paragraph 5.3 above so as to enable the Authority to respond

to a request for information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the EIR.

6.6 As between the parties, the Authority will determine at its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the FOIA or the EIR.

6.7 In no event will the Contractor respond directly to a request for information unless expressly authorised to do so by the Authority save to acknowledge receipt (if so requested by the Authority).

6.8 The Contractor acknowledges that the Authority may be obliged under the FOIA or the EIR to disclose Information without consulting with the Contractor, or following consultation with the Contractor and having taken its views into account.

6.9 The Contractor must ensure that all Information produced in the course of this Agreement or relating to this Agreement is retained for disclosure in line with the Authority's policy on information retention periods and must permit the Authority to inspect such records as requested from time to time.

6.10 The Contractor acknowledges that any lists or schedules provided by it outlining Confidential Information are of indicative value only and that the Authority may nevertheless be obliged to disclose Confidential Information.

7. Disclosures by the Authority

7.1 Nothing in this Agreement shall prevent the Authority disclosing any Information:

7.1.1 for the purpose of the examination and certification of the Authority's accounts; or

7.1.2 any examination pursuant to Section 6 (1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources; or

7.1.3 to any government department or any other contracting authority (as defined in The Public Contracts Regulations 2006). All government departments or contracting authorities receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other government departments or other contracting authorities on the basis that the information is confidential and is not to be disclosed to a Contractor which is not part of any government department or any contracting authority; or

7.1.4 to any person engaged in providing any services to the Authority for any purpose relating to or ancillary to this Agreement provided that in disclosing information the Authority discloses only the information which

is necessary for the purpose concerned and requires that the information is treated in confidence and that a confidentiality undertaking is given where appropriate.

8. Accessibility of Data

Where the Contractor is undertaking work on behalf of the Authority to develop new systems, practices or documentation in processing of data, the Contractor shall ensure that there remains the ability to extract data in a format accessible to and useable by the Authority (with regard to paragraph 10.3) supported by an Impact Assessment which is approved by the Authority.

9. Know-how

Nothing in this Agreement shall prevent either party from using any techniques, ideas or know-how gained during the performance of this Agreement in the course of its normal business, to the extent that this does not result in a disclosure of Information the subject of this Agreement.

10. Information Breaches

10.1 The Contractor shall ensure all losses or breaches of security or information are reported to the Authority within 1 working day whether actual, potential or attempted.

10.2 The Contractor will ensure all breaches are internally investigated, and appropriate remedial action taken, along with supporting the Authority and the Information Commissioner's Office in any investigation by it. A copy of the investigation report must be provided to the Authority.

10.3 The Contractor will immediately take all reasonable steps to remedy such breaches and to protect the integrity of both parties against any actual, potential or attempted breach or threat and any equivalent attempted breach in the future.

11. Breach, termination and continuance

11.1 The Contractor shall indemnify the Authority for any breach of the requirements of this schedule which renders the Authority liable for any costs, fines, claims or expenses under Legislation howsoever arising.

11.2 Failure on the part of the Contractor to comply with the provisions of this schedule shall amount to a breach of this contract and shall give the Authority the right to exercise any and all of the remedies in this contract and recover all costs incurred as a consequence of the Contractor's breach.

11.3 On termination of this Agreement howsoever arising the Contractor shall when directed to do so by the Authority, and instruct all its agents and subcontractors to:

11.3.1 transfer to the Authority the whole or any part of the Personal Data and other Information received or acquired by the Contractor for the purposes of or in the course of the delivery of the services the subject of this Agreement; and

11.3.2 ensure that such a transfer is made securely in a manner specified by the Authority and the data complies with the requirement at paragraph 7; and

11.3.3 securely destroy or erase the whole or any part of such Personal Data and other Information retained by the Contractor and provide to the Authority such proof of destruction as the Authority may reasonably specify.

11.4 The provisions of this paragraph shall continue in effect notwithstanding termination of this Agreement.