Data Protection & Confidentiality Policy

Version:	4
Consultation:	IG Advisory Committee Executive Committee
Ratified by:	Governance Committee
Date ratified:	15 December 2017
Name of originator/author:	John McIlveen
Date issued:	1 January 2018
Review date:	15 December 2020
Audience	All Trust employees, Governors, volunteers, contractors and Non Executive Directors

Version	Date	Reason for Change
3	November 2015	Routine review and update. Include information re Caldicott 2 and business continuity responsibilities. Updated job titles etc.
4	December 2017	Routine review and update. Include provisions of GDPR and National Data Guardian report on Data security, Consent and Opt-outs. Updated job titles and organisation names etc. Updated IG Committee structures following Governance Committee approval

1. POLICY STATEMENT

1.1 Everyone working for or on behalf of the NHS has a duty to keep information about patients, carers, clients, staff and other individuals confidential, and to protect the privacy of information about individuals. This duty is enshrined in law, in codes of practice issued periodically by the Department of Health, and in professional codes of conduct.

1.2 It is the policy of the Trust that the measures outlined in this policy should be followed by all employees, Governors, Non-Executive Directors, volunteers and contractors in order that compliance with legislation and good practice can be maintained.

2. INTRODUCTION

2.1 This document is a statement of Trust policy on Data Protection and Confidentiality. It includes guidance for staff on processing information in accordance with current legal obligations and best practice.

2.2 The Trust needs to collect and use information about people with whom it deals in order to operate. These include current, past and prospective patients, current, past and prospective employees, suppliers, clients/customers, and others with whom it communicates. In addition, it may occasionally be required by law to collect and process certain types of information to comply with the requirements of Government departments for business data.

2.3 For the purposes of this policy, the terms ‘data’ and ‘information’ are used interchangeably.

3. CONTEXT

3.1 The Data Protection Act (1998) defines a legal basis for the handling in the UK of information relating to living people. The General Data Protection Regulation, in force in the UK from 25 May 2018, updates the Data Protection Act and introduces new requirements for public authorities who handle personal data. The Confidentiality: NHS Code of Practice (published 2003) and the NHS Code of Practice - supplementary guidance: public interest disclosures (published Nov 2010) provide guidance concerning confidentiality for those who work for and on behalf of the NHS.

3.2 The Caldicott Guidelines focus specifically on the protection and processing of personal data within the NHS. The Trust maintains a firm commitment to these principles which are:

- Justify the purpose for collecting or holding personal data
- Do not use personal data unless it is absolutely necessary
- Use the minimum necessary personal
- Access to personal data should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- the duty to share personal data can be as important as the duty to respect service user confidentiality

3.3 The National Data Guardian's report *Data Security, Consent and Opt-outs*, published in July 2016, set out ten new standards of data security for the NHS, and made recommendations about how individuals might be better involved in and informed about how their information is shared.

3.4 Professional bodies (e.g. National Midwifery Council (NWC), General Medical Council (GMC)) provide additional supplementary advice and guidance for their own disciplines. These guidelines should not conflict with this Policy or legislative requirements.

4. PURPOSE

The purpose of this policy is:

- To ensure any personal information collected and held by the Trust is processed fairly and lawfully.
- To promote best practice in the processing of personal information.
- To ensure that Trust staff involved in processing personal information understand their responsibilities and obligations.
- To ensure that Trust staff responsible for the processing of personal information are adequately trained to fulfil their responsibilities and obligations.
- To outline the procedure for reporting and investigation of a suspected breach of Confidentiality and/or Data Protection.
- To provide assurance to our patients, staff and others with whom we deal that their personal information is processed lawfully and correctly and held securely at all times.

5. SCOPE

5.1 This policy relates to all types of information within the Trust. These include:

- Patient/Client/Service User information

- Personnel information
- Organisational information.

5.2 This policy covers all aspects of information, including (but not limited to):

- Storage, filing and record systems - paper and electronic
- Transmission of information – e-mail, post, telephone and fax
- Images, including CCTV and photographs

5.3 This policy applies to:

- all information systems purchased, developed and managed by, or on behalf of, the Trust
- All Trust employees (including those on fixed term contracts), non-executive Directors, Governors, contractors and volunteers
- Members of other organisations granted temporary or permanent access (for example to undertake audits or inspections) to confidential information held by the Trust.
- All systems provided by Third Party contractors, where the service has been negotiated on the Trust's behalf e.g. by Department of Health.

6. DUTIES

6.1 Chief Executive

The Chief Executive has overall responsibility for Information Governance which includes the Data Protection Act 1998. As the Accounting Officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

6.2 Caldicott Guardian

The Caldicott Guardian has a specific responsibility for reflecting patients' interests regarding the use of personal data. The Caldicott Guardian is responsible for ensuring that personal data is shared in an appropriate and secure manner. The Trust's Caldicott Guardian is the Medical Director.

6.3 Senior Information Risk Owner (SIRO)

The SIRO has Board level responsibility for the management of information risk within the Trust and the development and maintenance of Information Governance practices throughout the Trust including business continuity measures to ensure the safety and availability of information assets.

6.4 Trust Secretary

The Trust Secretary is responsible for the operational day to day management of all issues relating to Information Governance, including drafting policy documents, procedural guidance, training, audit and dealing with all IG related queries.

6.5 Data Protection Officer

Under the terms of GDPR the Trust must appoint a Data Protection Officer (DPO), who will inform and advise the Trust about its obligations to comply with the GDPR and other data protection legislation, and who will monitor compliance with those legal obligations. The DPO will manage internal data protection activities, advise on data protection impact assessments, and be the first point of contact for supervisory authorities and individuals whose data is processed.

6.6 Information Governance Officer

The Information Governance Officer offers advice to Trust staff on Information Governance matters, including Data Protection and Caldicott issues. The Trust Secretary and the Information Governance Officer are supported on day to day IG issues by the Assistant Trust Secretary.

6.7 Information Asset Owners

6.7.1 Information Asset Owners support the wider Information Governance agenda and may be members of the Trust's Information Governance Committee.

6.7.2 Information Asset Owners are responsible for:

- leading and fostering a culture that values, protects and uses personal data for the success of the Trust and the benefit of its service users;
- Identifying, and managing information flows within their team/service, for ensuring that each information flow is recorded in an Information Asset Register.
- identifying and keeping under review flows of personal data from their team/service;
- knowing who has access to that personal data, and why, and ensures that their use is monitored and complies with the law and with policy;
- ensuring that where appropriate, information sharing agreements are put in place to document the terms on which information is shared
- understanding and addressing risks to the personal data and providing assurance to the SIRO regarding business continuity in respect of that data;

6.8 Information Asset Administrators

Information Asset Administrators are responsible for supporting Information Asset Owners in ensuring the accuracy, security and lawful use of personal data within their own areas.

6.9 **All Staff**

6.9.1 It is the responsibility of each member of Trust staff to familiarise themselves with, and follow the policies relevant to their role/work.

6.9.2 All Trust staff, whether clinical or administrative, have responsibility for the safety and proper management of the information they process, and for the prompt reporting of any Information Governance incident using the Datix incident recording system.

6.9.3 All staff must complete their Information Governance refresher training annually.

6.10 **Information Governance Committee**

The Information Governance Committee (IGC) is a sub-committee of the Trust Board's Governance Committee. It comprises Information Asset Owners and key Information Governance staff, and managers with specific responsibilities in terms of the requirements of the Information Governance Toolkit, published by NHS Digital. The Committee is responsible for ensuring that the Trust establishes monitors and maintains appropriate integrated systems, processes and reporting arrangements for the management of all aspects of information governance, data protection and confidentiality. It supports and drives the broader information governance agenda and provides the Governance Committee and the Board with assurance that effective information governance best practice mechanisms are in place within the Trust.

6.11 **Head of Health Records**

The Head of Health Records will ensure oversee the management of health records in accordance with relevant Trust policies, and will ensure staff are provided with training for their responsibilities for record keeping. The Head of Health Records will facilitate timely access to health records where a legitimate subject access request has been received.

6.11 **Managers**

Managers should ensure through appraisal and regular supervision that staff are aware of and comply with key policies and procedures relevant to their work.

7. DEFINITIONS

7.1 **Staff**

Within this policy 'staff' is defined as including employees of the Trust, Non-Executive Directors, Governors, volunteers and contractors.

7.2 Personal data

Personal data is information that could be used in isolation or in combination with other items of information to identify a data subject directly or indirectly. It includes such items of data as:

Name, address, postcode, NHS Number, National Insurance Number
Family, Lifestyle or social circumstances
Education and Training details
Employment Details
Financial Details
Photographs and other images

7.3 Special categories of personal data

Any of the following data held by the Trust are considered to be special categories of personal data under the GDPR, and additional safeguards apply to processing these data:

Racial or ethnic origin
Political opinions
Religious or other beliefs
Trade union membership
Physical or Mental Health
Sexual life
Genetic data
Biometric data

Personal data regarding criminal convictions and offences are not included, but similar safeguards apply to processing these data.

7.4 Processing

Any of the following actions, in relation to the data, constitute processing: -

- Obtaining
- Accessing
- Recording
- Retrieval
- Consultation
- Holding
- Disclosing
- Sharing
- Using
- Transmission
- Erasure

- Destruction

7.5 **Data Subject**

Data Subject means an individual who is the subject of the personal data, either directly or can be identified from it. A data subject must be a living individual.

7.6 **Data Controller**

The Data Controller is the individual, company or organisation that determines the purpose and the manner in which personal data may be processed. [2]gether NHS Foundation Trust is the Data Controller.

7.7 **Data Processor**

Data Processor, in relation to personal data, means any other person other than an employee of the Trust who processes data on behalf of the Trust.

7.8 **Recipient**

Recipient, in relation to personal data, means any person to whom data are disclosed (including employees or agents of the Trust).

7.9 **Third Party**

Third party, means any person other than:

- the data subject
- the data controller
- any processor or other person authorised to process for the data controller

7.10 **Data protection legislation**

Within this policy, 'data protection legislation' shall be taken to mean the General Data Protection Regulation, the Data Protection Act 1998, or any subsequent UK legislation.

7.11 **Organisational information**

Organisational information means information other than personal information, (such as financial or business planning information, or minutes of confidential meetings) which may have a commercial value or which, if disclosed inappropriately, may disadvantage the Trust.

8 OWNERSHIP AND CONSULTATION

The Trust Secretary is the author and owner of this policy. The Information Governance Committee, and the Executive Committee have been consulted during the drafting of this policy.

9 RATIFICATION

This policy is ratified by the Governance Committee.

10 RELEASE DETAILS

This policy will be published on the Trust's intranet within the Information Governance pages.

11 REVIEW

This policy will be reviewed every 3 years, subject to changes in legislation, advances in technology or the production of national/regional guidance.

12 PROCESS FOR MONITORING COMPLIANCE

12.1 An overall assessment of compliance will take place on an annual basis through completion and publication of the Information Governance Toolkit (IGT), produced by NHS Digital. The Trust Board or its delegated Committee will give final approval for publication of the IGT. The IGT will be subject to an internal audit review as required by the NHS Operating Framework.

12.2 An annual IG report will be submitted to the Governance Committee. This report will include information on data protection performance and confidentiality breaches.

12.3 Electronic patient record systems will be subject to periodic audit to detect inappropriate access to confidential records. Audits will be undertaken or commissioned to assess wider information and IT security arrangements.

12.4 Managers will also monitor compliance within their work area, and take appropriate action when infringements of this policy are brought to their attention.

13 TRAINING

13.1 Guidance on confidentiality and data protection will be produced by the Trust Secretary and/or Information Governance Officer as required. This will include the creation and maintenance of Information Governance pages on the staff intranet, and associated documentation.

13.2 Training needs will be assessed by the Training Department and appropriate training provided. Such training will normally be through e-learning packages. All new staff will receive Information Governance awareness training as part of their corporate induction. Information Governance refresher training, also including data protection and confidentiality, will be a requirement for all existing

staff, and will form part of the Trust's suite of statutory and mandatory training, compliance with which will be monitored by the Delivery Committee.

13.3 Staff employment contracts will contain information highlighting individual responsibilities in respect of data protection and confidentiality. Examples of these clauses are shown in Appendix 1 of this policy.

14.0 POLICY PRINCIPLES

14.1 Legal requirements exist in relation to the collection, storage, accuracy, retention and disclosure of personal information. All processing of information by Trust staff must be carried out in accordance with principles set out in the Data Protection Act and any amending legislation, and with other relevant guidance such as that provided in the Caldicott guidelines, the Confidentiality: NHS Code of Practice, and this policy.

14.2 While Data Protection legislation applies to living individuals, where possible the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive.[1] The issues arising from the processing and provision of access to deceased persons' records can be complex and where these arise advice should be sought from the Head of Health Records or the Trust Secretary.

14.3 Individuals have certain rights regarding their personal data. These include:

- the right to be informed
- the right of subject access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated data processing

The Trust will ensure that procedures are in place to enable individuals to take advantage of all applicable rights regarding their personal data.

14.4 In addition to their rights under data protection legislation, individuals have a legal right to respect for private and family life under the Human Rights Act 1998. Staff must respect the dignity and right to confidentiality of service users when collecting and processing personal data. This includes the use of photographs and images, and the taking and sharing of images relating to patients for non-professional/non-clinical purposes is not permitted.

[1] Confidentiality: NHS Code of Practice 2003 and the NHS Code of Practice - supplementary guidance: public interest disclosures (2010)

14.5 The Trust will undertake data protection impact assessments where appropriate, to further its intention of achieving data protection by design and by default.

14.6 The Trust will process personal data and special categories of personal data only where there is a valid legal basis for doing so under GDPR or any equivalent UK legislation. Where special categories of personal data are processed for some specific purposes as set out under GDPR or any equivalent UK legislation, the Trust will where relevant produce and retain appropriate policy documents setting out in relation to that processing the Trust's processes for maintaining compliance with the conditions for processing, and the retention periods applicable to that data.

14.7 The Trust will maintain a record of its processing activities, in a format which complies with requirements set out in GDPR or any equivalent UK legislation.

15 TRANSFER OF PERSONAL DATA

15.1 Any transfer of personal data must be carried out securely with an adequate level of protection given to the data in transit in accordance with current NHS information security standards. This applies both to the transfer of paper-based information, as well as to data transferred via electronic means, (including email and portable devices such as memory sticks). The Trust's Information Security Policy provides guidance on the secure transmission of personal data. It is recommended that users contact the IT department before considering the transmission of any significant amounts of personal data to ensure they are using the most appropriate and secure mechanism.

15.2 No personal data may be transferred outside the UK or the European Union without the agreement of the Trust Secretary. Transfers of personal data outside the EU or UK will take place only where the Trust receives assurance that an equivalent level of data protection applies in the receiving country as that provided in the UK. Safeguards must be in place to ensure that personal data is handled, stored and transmitted securely, regardless of the destination.

15.3 Advice should be sought from the Trust Secretary before transferring any personal data for the first time, regardless of the destination.

16 ACCESS TO AND DISCLOSURE OF PERSONAL INFORMATION

16.1 Care must be taken to ensure any access to or disclosure of personal or sensitive information is for an authorised purpose. Anyone in doubt as to whether a disclosure of information is authorised should check with their manager.

16.2 Data subjects will have a right of access to their information. Requests from patients or their representatives to access their health records must be made in

writing, and should be handled in accordance with the guidance contained in the Trust's Access to Health Records Policy.

16.3 No information relating to patients should be given over the telephone unless the person communicating the information is sure that the person they are speaking to is entitled to receive the information (e.g. a GP Practice).

16.4 Personal information will usually be disclosed only if the individual has given their consent to the disclosure. However, under certain circumstances, the Trust has a power or an obligation to disclose personal information without the individual's consent, (for example to assist the police in preventing or detecting crime, or where a court order is produced). Where the Trust has a power to disclose information without consent, that power will be exercised only if members of the public, patients or staff are at serious risk.

16.5 Requests for information by the police will be considered only where such requests are in the form of a fully completed Data Protection request form. If the request is deemed appropriate by the Trust Secretary and the Head of Health Records, the Health Records Department will process the request.

16.6 When a decision to release information to the police is made only the minimum necessary information to meet the identified need will be provided. Advice should be sought from the Trust Secretary (who will refer to the Caldicott Guardian for complex matters) in respect of all requests for patient/staff information from the police.

16.7 Where the Trust has an obligation to disclose information without consent, (for example, where required by legislation or by a Court Order), such disclosures must be approved in advance by the relevant Director or by the Trust Secretary.

17 INFORMATION SHARING

17.1 Where the Trust shares information with other organisations (for example for the provision of care or for safeguarding purposes) Information Asset Owners should maintain a record of those organisations and the nature of the information shared. Where appropriate, an Information Sharing Agreement should be drawn up to cover the type of information to be shared, the circumstances and frequency under which information is shared, and any safeguards surrounding transfers of information.

17.2 Information will not be shared for purposes beyond direct care where an individual has exercised the right to opt out of sharing information for this purpose, unless there is a mandatory legal requirement or an over-riding public interest in sharing that information.

18 ACCESS TO IT SYSTEMS

18.1 Access to systems that hold sensitive or other confidential information relating to patients or staff must be strictly controlled. The Trust IT Security Policy provides detailed guidance on implementing access control to IT systems.

18.2 Key standards are:

- Restrict access to a level appropriate to the user's role.
- Access should only be gained by means of a restricted login and, where necessary, a security password or pin number, which is issued when the appropriate training has been received and the relevant level of access has been authorised.
- Passwords must be kept secure and never shared with other users. Password sharing is treated seriously and may lead to disciplinary action.
- Users must exit to the appropriate sign-on screen when the computer is not in use.
- No computers should be placed in such a position that unauthorised persons can view patient or other confidential information. If this proves to be impossible, the purchase of a privacy filter should be considered.

18.3 In some circumstances generic logins to PCs (i.e. the Windows desktop) are allowed (for example shared PCs in ward areas) but access to applications that contain personal data must only be made using individual username/password and/or pin.

18.4 Personal data relating to service users, their families and carers must be processed only on devices issued by the Trust.

19 INAPPROPRIATE ACCESS TO RECORDS

19.1 Access to data for which the member of staff does not have authorisation, **at the time the record is** accessed, is prohibited. This includes access to his/her own information without a formal request

19.2 Any staff accessing or attempting to access records they are not authorised to see may be subject to disciplinary procedures. Unauthorised access to or disclosure of information may also render the individual responsible liable to prosecution.

20 STORAGE AND DISPOSAL OF INFORMATION

20.1 All printed material containing personal data or confidential organisational information must be treated as confidential and kept secure at all times. Personal data stored electronically must be stored only on devices that have adequate security measures in place. (See Trust IT Security Policy)

20.2 All data (manual and electronic) should be periodically reviewed to ensure that the information is accurate, up to date and complete.

20.3 No data (manual and electronic) should be kept for longer than is necessary. Data will be retained in accordance with the retention periods set out in the Records Management Code of Practice for Health and Social Care 2016.

20.4 All printed material containing personal data or confidential organisational information must be disposed of securely using the confidential waste disposal service provided by the Trust. The disposal of computer equipment and devices capable of storing information should be carried out through the IT department to ensure all data is removed before disposal.

21 CLINICAL RESEARCH

21.1 All research studies must have full Research & Development approval in writing prior to commencing. As part of the R&D approval process, data protection approval will be sought. R&D approval will be issued only on confirmation of data protection approval and a favourable opinion from the Research Ethics Committee and MHRA (where applicable).

21.2 Researchers who are not Trust staff are required to have an honorary contract prior to starting their research project, when their conduct, for the purposes of the research, could foreseeable, directly affect the type, quality or extent of prevention, diagnosis or treatment of illness or cause foreseeable injury or loss to an individual to whom the organisation has a duty of care. Proof of a Trust contract is required before data protection approval and thus R&D approval is given.

22 REPORTING BREACHES OF CONFIDENTIALITY

22.1 All information governance incidents, including actual and suspected breaches of confidentiality, must be recorded on Datix.

22.2 The Trust Secretary will review each report and if necessary request an investigation by the appropriate department/manager. This may include the Trust Secretary or Caldicott Guardian commissioning an audit of the records accessed by a staff member on one or more electronic record systems. Where appropriate, an investigation may be deemed to warrant disciplinary action. This will be the responsibility of the local line manager or the Human Resources Department.

22.3 Where a breach occurs which presents a risk to the confidentiality of a person's data, the data subject will be informed of that breach without undue delay. Where appropriate, breaches will be reported externally (for example to the Information Commissioner, or within the Annual Report as applicable), using the relevant reporting mechanism.

23 COMPLAINTS ABOUT CONFIDENTIALTY.

23.1 The Trust will deal with complaints about its confidentiality processes within the spirit of the Trust's Complaints Policy and Procedure. However, complainants also have the right to complain to the Information Commissioner, but usually this is only when the local complaints process has been exhausted. For more information please refer to the Information Commissioners website.

24 BREACH OF THIS POLICY

24.1 Failure to manage personal data securely places the Trust at risk of breaching data protection legislation, NHS Caldicott Guidelines and Trust policy. All Trust staff have responsibility for the security and proper management of the personal data and other confidential information they process.

24.2 Failure to comply with the terms of this and associated policies may lead to disciplinary action and / or legal proceedings against the individuals concerned.

25 REFERENCES

- The Caldicott Guardian Manual
- National Data Guardian's *Review of Data Security, Consent and Opt-Outs*
- NHS Information Governance - Guidance on Legal and Professional Obligations
- Data Protection Act 1998.
- General Data Protection Regulation
- The common law duty of confidence.
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- IT Security Policy
- Information Security Policy
- E-mail and Internet Policy
- Information Governance Framework Policy
- Disciplinary Policy
- Access to Health Records Policy
- Health and Social Care Records Policy and Procedure
- Records Management Code of Practice for Health & Social Care 2016
- Mobile Working Policy
- Policy on Social Media
- Confidentiality: NHS Code of Practice
- NHS Code of Practice - supplementary guidance: public interest disclosures (2010)

APPENDIX 1 – Staff employment contract clauses

The staff contract includes a statement of confidentiality as follows:

STANDARDS OF CONDUCT

- You are bound by the provisions of the Standards of Business Conduct published from time to time by the NHS Executive. You are directed to read these standards.
- All staff must abide by the Trust's Standing Financial Instructions.
- Personal information recorded on computer is governed by the Data Protection Act and unauthorised disclosure of such information is unlawful.

CODE OF CONFIDENTIALITY

- You will respect the rights of our patients/clients/staff/volunteers right to privacy, including information such as their names, addresses, background, family relationships and nature of their problems.
- You will limit your discussions to the information required to execute your duties effectively and ensure those discussions are carried out in an appropriate setting.
- You will ensure that you will take all reasonable measures to keep confidential any identifiable information that comes in to your possession or control including computerised, manual, recorded or verbal information.
- You must not disclose any confidential information to any person except authorised personnel. However there may be rare occasions when the disclosure of confidential information is appropriate. Advice should always be sought from your manager or professional advisor before disclosure takes place.
- You must only use or reproduce confidential information for the purpose for which it was collected.
- You must not permit unauthorised persons to gain access to confidential information which is in your possession or control, when it is stored, transmitted, received or disposed of.
- You understand that the need for confidentiality continues even when you cease to be an employee/volunteer.

Individual Responsibilities

- In the course of their work many employees are routinely called on to handle and process person-identifiable information whether it is stored on paper or on computer. They are responsible for safeguarding the confidentiality of all personal and Trust information, transmitted or recorded by any means. Such information must not be discussed or disclosed, except to authorised personnel.