DATA PROTECTION AND CONFIDENTIALITY POLICY

<table>
<thead>
<tr>
<th>CATEGORY:</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASSIFICATION:</td>
<td>Governance</td>
</tr>
<tr>
<td>PURPOSE:</td>
<td>The purpose of this policy and its associated documents is to ensure that the Trust complies with the Data Protection Act 1998 (DPA), the Caldicott principles and the duty of confidentiality in relation to all personal data held.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controlled Document Number:</th>
<th>838</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Number:</td>
<td>2</td>
</tr>
<tr>
<td>Controlled Document Sponsor:</td>
<td>Director of Corporate Affairs</td>
</tr>
<tr>
<td>Controlled Document Lead:</td>
<td>Senior Manager Information Governance</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Chief Executive</td>
</tr>
<tr>
<td>On:</td>
<td>January 2015</td>
</tr>
<tr>
<td>Review Date:</td>
<td>December 2017</td>
</tr>
<tr>
<td>Distribution:</td>
<td>All staff</td>
</tr>
<tr>
<td></td>
<td>All staff</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Policy Statement</td>
</tr>
<tr>
<td>2</td>
<td>Scope</td>
</tr>
<tr>
<td>3</td>
<td>Framework</td>
</tr>
<tr>
<td>4</td>
<td>Duties</td>
</tr>
<tr>
<td>5</td>
<td>Implementation and Monitoring</td>
</tr>
<tr>
<td>6</td>
<td>References</td>
</tr>
<tr>
<td>7</td>
<td>Associated Policy and Procedural Documentation</td>
</tr>
</tbody>
</table>

### Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>Schedules 2 and 3 of the Data Protection Act</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Caldicott Principles</td>
</tr>
</tbody>
</table>
Policy Statement

1.1 The purpose of this policy and its associated documents is to ensure that the Trust complies with the Data Protection Act 1998 (the DPA), the Caldicott principles and the duty of confidentiality in relation to all personal data held.

1.2 The Trust has a legal obligation to comply with all appropriate legislation in respect of personal data and the common law duty of confidentiality. It also has a duty to comply with guidance issued by the Department of Health and the Information Commissioner in relation to the use of personal data.

1.3 The Trust is committed to protecting the rights and privacy of individuals (including staff, patients, contractors, members of the public and any other groups) in accordance with the DPA to which it is subject as a controller and processor of personal data (data controller).

1.4 The Trust may need to process information about its staff, its patients and other individuals for legitimate reasons in the discharge of its everyday business, for example in the provision of healthcare and for employment reasons. Such information must be collected, handled, used, stored, shared and disclosed fairly and lawfully.

Scope

2.1 This policy applies to all areas and activities of the Trust and to all individuals employed by the Trust including contractors, volunteers, students, locum and agency staff and staff employed on honorary contracts.

2.2 This policy covers the processing of all personal data held by the Trust, in any format including paper and electronic information. Personal data is defined as any data relating to an individual who is, or can be identified either from the data, or from the data in conjunction with other information that is in, or is likely to come into the possession of the data controller. This would include data such as a person’s name, address, date of birth, hospital number, NHS number, national insurance number. In addition there is a second category of data referred to as ‘sensitive personal data’ this includes data such as health data, ethnicity, religion, trade union status, sexual preferences, criminal record or race.

Framework

3.1 This section describes the broad framework for the Data Protection and Confidentiality Policy. Detailed instructions are provided in the associated procedural documents.

3.2 The Director of Corporate Affairs shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.
3.3 The Trust will meet its obligations to comply with the DPA and other guidance and standards of confidentiality and information security through this policy and the monitoring of it by:

3.3.1 ensuring that all members of staff are aware of, understand and fully comply with the Data Protection Act 1998

3.3.2 ensuring that all members of staff, with responsibility for processing patient-identifiable information, are aware of and comply with the Caldicott principles

3.3.3 ensuring that all members of staff are aware of the Department of Health Publication, Confidentiality: NHS Code of Practice, 2003 which sets out individual and organisational responsibilities covering both confidentiality and the Data Protection Act 1998

3.3.4 ensuring that the Trust has procedures in place to mitigate data protection and information security breaches, to demonstrate assurance regarding business continuity, and comply with records management requirements.

3.4 The Trust recognises the need to share personal information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient. The Trust will obtain and share information in accordance with the common law duty of confidence, Article 8 of the Human Rights Act 1998 (right to respect for private and family life), the DPA and the Caldicott Principles.

3.5 The Data Protection Act

The DPA is the key piece of legislation covering security and confidentiality of personal information. The eight principles of the DPA are set out below:

3.5.1 Personal data shall be processed fairly and lawfully

3.5.2 Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3.5.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.5.4 Personal data shall be accurate and, where necessary, kept up to date.

3.5.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

3.5.6 Personal data shall be processed in accordance with the rights of data subjects under the DPA.
3.5.7 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.

3.5.8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless 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.

3.6 Principle 1 of the DPA states that personal data shall be processed fairly and lawfully and shall not be processed unless –

3.6.1 at least one of the conditions in Schedule 2 is met, and
3.6.2 in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met
3.6.3 Further information regarding the conditions in schedule 2 and 3 is set out in Appendix A.

3.7 Caldicott
Caldicott principles are a set of principles specific to the use of patient data within the NHS and sets out seven best practice principles, further information can be found at Appendix B:

3.7.1 Justify the purpose(s) of using confidential information
3.7.2 Do not use patient-identifiable information unless it is absolutely necessary
3.7.3 Use the minimum necessary patient-identifiable information that is required
3.7.4 Access to patient-identifiable information should be on a strict need-to-know basis
3.7.5 Everyone with access to patient-identifiable information should be aware of their responsibilities
3.7.6 Understand and comply with the law
3.7.7 The duty to share information can be as important as the duty to protect patient confidentiality

3.8 Duty of confidence
3.8.1 A duty of confidence arises where one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is:

a) A legal obligation derived from case law
b) A requirement established within professional codes of conduct

c) Included within all NHS staff members contracts of employment

3.8.2 Patients entrust staff with sensitive information regarding their health and other matters as part of their treatment. They do so in confidence and have the legitimate expectation that staff will respect their privacy and act appropriately. It is essential that the trust of patients is retained and that the Trust provides and is seen to provide, a confidential service.

3.8.3 Breach of confidence, including inappropriate accessing, disclosure or use of health or staff records, or abuse of computer systems may lead to disciplinary measures, bring into question registration and possibly result in legal proceedings. Staff should ensure that they are aware of the requirements and standards of behaviour that apply.

3.9 Security of personal information

All information relating to identifiable individuals and any other information that may be deemed sensitive (such as commercially sensitive information), must be kept secure at all times. The Trust shall ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction or damage to this information. The Trust will maintain related policies on the transfer and storage of personal information and the use of electronic and mobile media. Further information can be found in:

- the Employees Guide to Data Protection and Confidentially, the Information Governance Policy and
- the Information Security Policy.

All staff have a responsibility to ensure that all personal data is stored securely at all times, in particular staff must ensure that:

3.9.1 Paper information is used appropriately to prevent loss or accidental disclosure. All paper documents which contain personal information of staff or patients, such as handovers, must be stored securely at all times and not taken outside of the Trust. Further information is available in the Use of Paper Records (including handover) Procedure.

3.9.2 Electronic information is stored in a secure manner, staff are not authorised to store personal data of Trust employees or patients personally, e.g. on their personal/home computer, laptop, or other type of removal media, or within their personal email account.

3.9.3 All electronic information must be stored on the Trust network and not on the hard drive of specific computers. Where information is held on removable media the media must be
encrypted. In accordance with the Information Security Policy all Trust laptops will be encrypted and staff are only permitted to transfer data to Trust approved encrypted USB. All USB ports on all pcs have been blocked to prevent the downloading of data to any device not approved by the Trust. In specific circumstances staff may be granted the ability to write to other types of media as outlined in the Information Security Policy.

3.9.4 When personal information is sent by post care must be taken to ensure the correct information is sent to the correct person.

3.9.5 When personal information is sent by fax the Trust Fax Procedure must be followed.

3.9.6 When personal information is sent by email it must be sent in accordance with the Information Security Policy.

3.9.7 All transfers of information out of the UK must be carefully considered, in all cases the Senior Manager Information Governance must be consulted before any personal information is sent outside of the UK.

3.10 Access to information

3.10.1 Staff access to personal information is restricted; Staff should only have access to personal information or create records containing personal information in the following circumstances:

- For health care, where the staff member has a legitimate relationship with a patient i.e. the staff member is currently involved in providing care to the patient, or is a member of the health care team responsible for treating the patient. This description includes both health care professionals and administrators e.g. ward clerks, medical secretaries and receptionists.

- For HR issues, where the staff member is the line manager of another staff member, or is authorised to access personal files e.g. HR department, department administrator etc. Where the staff member is authorised to access personal data/create records in specific circumstances where there is a justified reason for doing so, for example:

  a) Legal services staff, or complaints staff accessing patient information for medico-legal cases and complaint

  b) Clinical auditors accessing patient information for use in registered audits

  c) Clinical coding staff accessing information for coding purposes

  d) Medical records team accessing information as part of their duties, e.g. booking clinics.
e) Informatics and Finance staff accessing information for charging purposes
f) Data Quality team accessing information for identifying data quality errors
g) IT staff who are responsible for maintaining IT systems.
h) Communications staff to provide information in line with the Media Policy

3.10.2 This list is not exhaustive, however staff are prohibited from accessing, or using patient information for personal reasons, or where there is no justification for doing so, e.g. accessing information of family members, friends, celebrities, colleagues or neighbours, where they are not involved in that persons care within the Trust.

3.10.3 Examples of inappropriate access could include staff accessing information of patients where:

a) The patient was not at any time under the care of the staff member
b) The staff member has no work related reason to access the record
c) The staff member accessed the record for personal reasons without consent from the Trust

3.10.4 Staff who are patients of the Trust must not access medical information the Trusts holds in relation to them as patients, such requests must be dealt with by the Medical Records Department in accordance with the Subject Access Policy, refer to 3.13 of this policy.

3.11 Use of Information

3.11.1 Use of information for audit or research

Patient information must be used in accordance with the DPA and the duty of confidentiality, staff members must not use patient information for non – healthcare purposes, such as audit or research unless that audit or research project has been approved by the relevant Departments. Research projects must be carried out in accordance with the Policy on Research Governance and audit must be carried out in accordance with the Clinical Audit Policy and Procedure.

3.11.2 Use of information for teaching or publication

Staff must not use patient data for other reasons such as teaching or publication without the express consent of that patient. For information on the use of images please refer to the Trust Photographic and Video Recording Consent and Confidentiality policy and procedure.
3.12 Disclosure of information
Staff members must not disclose the personal data of patients to third parties without express permission from the patient, or where there is a legally justified reason as to why the disclosure should be made e.g. disclosure to the Coroners Office or in the patients best interests e.g. for safeguarding reasons in accordance with the Safeguarding Policy and Procedure. Care must be taken when discussing patients with relatives, or when telephone calls are made or received. Further information is available in the Employees Guide to Data Protection and Confidentiality.

3.13 Subject access requests
The DPA provides individuals with the right to request access to records held about them. Requests from patients/relative/third parties for copies of medical records must be dealt with by the Medical Records Department. Please refer to the Access to Health Records Procedure.

3.14 Sharing information
The Trust is required to share information about patients, for various reasons. When information is shared with non-NHS organisations, or for non-healthcare reasons generally patient consent must be obtained and an information sharing protocol may be needed. Please seek advice from the Senior Manager Information Governance. All information sharing protocols must be logged with the Corporate Risk and Compliance Unit and signed by the Senior Information Risk Owner if the data does not relate to patients or the Caldicott Guardian if patient data is being shared.

3.15 Ownership of data
Personal information of patient and staff members of the Trust remains the Trust property. Staff members are not permitted to store staff or patient information on their own personal/non-Trust devices such as laptops, home computers, discs or USBs. Personal data may be transferred to a Trust device such as a laptop or USB provided there is justification for doing so. All Trust devices are encrypted to protect the data in the event of loss or theft. The data must remain on the secure device; staff must not transfer personal information from a secure device to a personal non-encrypted device.

3.16 Destruction/disposal of data
3.16.1 Confidential data must be destroyed in a secure manner. All information held by the Trust must be destroyed in accordance with the Record Management and Information Lifecycle Policy.

3.16.2 Any information held in a paper format must be destroyed via the blue confidential waste bags.
3.16.3 Where confidential Information is held on removable media and the removable media needs to be destroyed or replaced this must be destroyed in accordance with the Information Security Policy.

3.16.4 For secure disposal of other types of media, such as fax/printer ribbons, please contact the Senior Manager for Information Governance for advice on disposal.

4 Duties

4.1 Chief Executive
The Chief Executive has overall responsibility for data protection within the Trust. As accountable officer he/she is responsible for ensuring the Trust complies with the Data Protection Act.

4.2 Caldicott Guardian
The Trust’s Caldicott Guardian has particular responsibility for reflecting patient’s interests regarding the use of patient identifiable data. He/she is responsible for ensuring that patient identifiable data is used and shared in an appropriate and secure manner. The Trust's Executive Medical Director is the Trust's appointed Caldicott Guardian.

4.3 Director of Corporate Affairs Senior Information Risk Owner (SIRO)
The Director of Corporate Affairs is the named director responsible for data protection. The Director of Corporate Affairs will provide assurance to the Board of Directors on compliance with this policy. The Director of Corporate Affairs is the Senior Information Risk Owner. The SIRO is the owner of the Trust's Information Asset Register. For more information please refer to the Information Asset Guidance document.

4.4 Information Asset Owners (IAO)
Information Asset Owners (IAOs) are accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they own.

4.5 Information Asset Administrators (IAA)
Information Asset administrators have day to day responsibilities for control of information assets.

4.6 Senior Manager Information Governance
The Senior Manager Information Governance is responsible for ensuring that the DPA, Caldicott principles and duty of confidentiality are fully observed, specifically he/she is responsible for:
4.6.1 ensuring that training is available to staff in accordance with the Mandatory and Statutory Training Policy

4.6.2 ensuring compliance with requirements from the Information Commissioners Office, including notification

4.6.3 Advising on and updating policies in relation to guidance from the ICO, Department of Health or other relevant organisations

4.6.4 Raising awareness of data protection and confidentiality issues to staff of all levels

4.6.5 Providing guidance to staff regarding legislation, relevant policies, procedures and good practice

4.6.6 Ensuring data protection and confidentiality breaches are investigated in conjunction with the relevant Operational Division.

4.7 All Managers are responsible for ensuring that:

4.7.1 Staff are aware of and adhere to this policy

4.7.2 This policy is built into local processes

4.7.3 Any breaches, or suspected breaches, of data protection or confidentiality are reported in line with the Trusts’ Incident reporting procedure.

4.8 All staff

All staff must:

4.8.1 Comply with the Data Protection Act, Caldicott principles, the common law duty of confidentiality, this policy and associated procedures

4.8.2 All staff must adhere to the standards set out in the NHS Code of Practice on Confidentiality, which is a guide to the required practice for those who work within or under contract to the NHS

4.8.3 All staff must ensure compliance with the terms of their contract of employment, which includes clauses in relation to confidentiality and data protection.

4.8.4 Health professionals working in the NHS are bound by professional codes of conduct in respect of confidentiality

4.8.5 Staff are responsible for ensuring that any breach, or suspected breach, of this policy is reported via the online incident reporting system and in accordance with the Trust’ Incident reporting procedures.
5 Implementation and Monitoring

5.1 Implementation

5.1.1 This policy will be available on the Trust's Intranet Site. The policy will also be disseminated through the management structure within the Trust;

5.1.2 All staff will receive training in data protection and confidentiality on an annual basis through information governance mandatory training sessions.

5.2 Monitoring

5.2.1 Monitoring of compliance with the policy will be undertaken using the Information Governance Toolkit Assessment. This is a self assessment completed annually, which is signed off by the Information Governance Group and the Board of Directors. Evidence will be collected to support the standards and an annual report regarding the process for sign off will be made to Audit Committee.

5.2.2 Compliance with the policy will be further monitored by the Information Governance Group, who will receive a report of all incidents where breaches of data protection, confidentiality and Caldicott have occurred within the Trust.

6 References

6.1 Legislation

Data Protection Act 1998
Access to Health Records 1990
Access to Medical Reports Act 1988
Human Rights Act 1998
Freedom of Information Act 2000
Crime and Disorder Act 1998
Computer Misuse Act 1990
Criminal Justice and Immigration Act 2008

6.2 NHS and related guidance

Confidentiality: NHS Code of Practice
Records Management: NHS Code of Practice
Information Security Management: NHS Code of Practice
Employee Code of Practice (Information Commissioner)
Caldicott Report 1997
Caldicott Review 2013

7 Associated Policy and Procedural Documentation

Information Governance Policy
Information Security Policy
Record Management and Information Lifecycle Policy
Freedom of Information and EIR Policy
Photographic and Video Recording Consent and Confidentiality Policy and Procedure
Mandatory and Statutory Training Policy
Data Quality Policy
Policy for the Reporting and Management of Incidents, Including Serious Incidents Requiring Investigation
Media Policy
Clinical Audit Policy and Procedure
Fax Procedure
Use of Paper Information (including handovers) Procedure
General Policy on Research Governance
Safeguarding Policies
Access to Health Records Procedure
Information Asset Guidance
Appendices

Appendix A – Schedule 2 and 3 of the Data Protection Act

The conditions set out in Schedules 2 and 3 to the Data Protection Act are known as the “conditions for processing”. Organisations processing personal data need to be able to satisfy one or more of these conditions. This will not, on its own, guarantee that the processing is fair and lawful – fairness and lawfulness must still be looked at separately.

The conditions for processing are more exacting when sensitive personal data is involved, such as information about an individual’s health or criminal record.

Full information can be found here:

Schedule 2

Schedule 3

A brief summary is set out below

Schedule 2 for personal data

- The individual who the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's “vital interests”. This condition only applies in cases of life or death, such as where an individual’s medical history is disclosed to a hospital’s A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the “legitimate interests” condition.
Schedule 3 for sensitive personal data

- The individual who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:
  - the individual (in a case where the individual’s consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual’s consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of individuals.
Appendix B

The Caldicott Principles

1. Justify the purpose(s) of using confidential information

Every proposed use or transfer of patient-identifiable information within or from an NHS organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by the information governance team.

2. Do not use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential and there is no other alternative for that purpose. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary patient-identifiable information that is required

Where use of the patient-identifiable is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for to achieve the purpose.

4. Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

5. Everyone with access to patient-identifiable information should be aware of their responsibilities

All staff handling patient-identifiable information - both clinical and non-clinical staff – should be fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law

Every use of patient-identifiable information must be lawful.

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