# Data Protection & Confidentiality Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>November 2015</td>
<td>Routine review and update. Include information re Caldicott 2 and business continuity responsibilities. Updated job titles etc.</td>
</tr>
</tbody>
</table>
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 the principles and legal obligations outlined in the Data Protection Act (1998) and how to comply with best practice for information handling as described in the Confidentiality: NHS Code of Practice and the Caldicott Report of 1997.

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 Confidentiality: NHS Code of Practice (published 2003) and the NHS Code of Practice - supplementary guidance: public interest disclosures (published Nov 2010) provides a guide to required practice concerning confidentiality for those who work for and on behalf of the NHS.
3.2 The Caldicott Report of 1997 focused specifically on the protection and processing of patient identifiable information within the NHS. The Trust maintains a firm commitment to the principles stated within the report which are:

- Justify the purpose for collecting or holding patient-identifiable information
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law

3.3 A review of information sharing carried out in 2013 resulted in a new Caldicott Report which expands the principles in the original report to include health, social care and local authorities. The report added a seventh Caldicott principle:

- the duty to share personal confidential data can be as important as the duty to respect service user confidentiality

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 patient identifiable information. The Caldicott Guardian is responsible for ensuring that patient identifiable information 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 Director of Service Delivery has overall 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 **Information Governance Officer**

The Information Governance Officer offers advice to Trust staff on Information Governance matters, including Data Protection and Caldicott issues.

6.6 **Information Asset Owners**

6.6.1 IAOs are senior members of Trust staff. Their role is to understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO on the security and use of these assets. Information Asset Owners are responsible for overseeing wider information governance practice in their own areas. Information Asset Owners support the wider Information Governance agenda through their membership of the Trust’s Information Governance and Health Records Committee.

6.6.2 In particular the IAO must:

- lead and foster a culture that values, protects and uses information for the success of the Trust and the benefit of its service users;
- know what information the asset holds, what enters and leaves it and why;
- know who has access, and why, and ensures that their use is monitored and complies with policy;
- understand and address risks to the asset and provide assurance to the SIRO regarding business continuity;
- ensure that the asset is fully used for the benefit of the Trust and its service users, including responding to requests for access from others.

6.7 **Information Asset Administrators**

Information Asset Administrators are responsible for ensuring the accuracy of information within their own areas, under the supervision of the relevant Information Asset Owner.
6.8 **All Staff**

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

6.8.2 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 **Information Governance and Health Records Committee**

The Information Governance and Health Records Committee is a sub-committee of the Trust Board’s Governance Committee. It comprises Information Asset Owners and key Information Governance staff, and 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 and data protection and confidentiality. It will support and drive the broader information governance agenda and provide the Governance Committee and the Board with assurance that effective information governance best practice mechanisms are in place within the organisation.

6.10 **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 access to health records where a legitimate subject access request under the Data Protection Act 1998 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 Information**

Personal information is information that could be used in isolation or in combination with other items of data 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 **Sensitive Personal Information**

Any of the following data held by the Trust are considered to be sensitive data within the Data Protection Act:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade union membership
- Physical or Mental Health
- Sexual life
- Alleged offences
- Criminal proceeding or convictions

7.4 **Processing**

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

- Obtaining
- Accessing
- Recording
- Retrieval
- Consultation
- Holding
- Disclosing
- Use
- 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. *geth*er 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 **The Act**

Within this policy, ‘The Act’ shall be taken to mean the Data Protection Act 1998.

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 and Health Records Committee has been consulted during the drafting of this policy.

9 **RATIFICATION**

This policy is ratified by the Senior Information Risk Owner.

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 2 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 Information Governance Toolkit (IGT), which is sponsored by the Department of Health, and which includes a module on Confidentiality and Data Protection Assurance. The Trust Board or its delegated Committee will give final approval for publication of the IG Toolkit.

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 which includes training and awareness of data protection and confidentiality requirements. 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 The Data Protection Act contains 8 Principles of Data Protection that describe legal requirements in relation to the collection, storage, accuracy, retention and disclosure of personal information. These principles are set out in Appendix 2 of this policy. All processing of information by Trust staff must be carried out in accordance with these principles, and with other relevant guidance such as that provided in the Caldicott Report, the Confidentiality: NHS Code of Practice and this policy.

14.2 Although the Data Protection Act (1998) does not apply to deceased persons, 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. 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 Trust Secretary or the Head of Health Records.

14.3 The Data Protection Act 1998 gives individuals certain rights regarding their personal data. These include the right to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access. (See Appendix 3). Other individual rights are listed in Appendix 4. The Trust will ensure that procedures are in place to enable individuals to take advantage of their rights under the Data Protection Act.

14.4 In addition to the Data Protection Act, individuals also 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 identifiable information. This includes the use of photographs and images, and the taking and sharing of images relating to patients for non-professional/clinical purposes is not permitted.

15 TRANSFER OF IDENTIFIABLE INFORMATION

15.1 Any transfer of identifiable 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), which may require the use of encryption software in order to guarantee security in transit. The Trust’s Information Security Policy provides guidance on the secure transmission of identifiable data. It is recommended that users contact the IT department before considering the transmission of any significant amounts of patient identifiable data to ensure they are using the most appropriate and secure mechanism.

15.2 Any data containing identifiable information will only be transferred by the Trust outside the UK for processing if it is securely encrypted during transit and the Trust is satisfied that, taking into account all the circumstances of the transfer, an adequate level of protection to the data as that provided in the UK is ensured.

15.3 Advice should be sought from the Trust Secretary before transferring any identifiable data for the first time.

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 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 Information relating to patients, including communication of test results should not be given over the telephone unless the person communicating the information can ensure they are speaking to someone entitled to receive the information e.g. 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 the power 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). Information will only be released in these circumstances if members of the public, patients or staff are at serious risk or if a court order is produced.

16.5 The police must produce a Data Protection request form for any information to be released. This must be provided to the Trust Secretary. If the request is deemed appropriate, the Trust Secretary will pass the request to the Head of Health Records who will then 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 Unauthorised access to or disclosure of information may result in disciplinary action and may render the individual responsible liable to prosecution.
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.

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 patient identifiable data must only be made using individual username/password and/or pin.

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.

20 STORAGE AND DISPOSAL OF INFORMATION

20.1 All records, reports, printouts or other printed material containing identifiable or confidential organisational information must be treated as confidential and kept secure at all times. Identifiable 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 or system held) should be periodically reviewed to ensure that the information is accurate, up to date and complete.

20.3 All data (manual and system held) should not be kept for longer than is necessary. The Trust’s Records Management Policy provides guidance on minimum retention periods and disposal of records.

20.4 All reports, printouts or other printed material containing identifiable or confidential organisational information must be disposed of securely. The Trust provides a secure confidential waste disposal service which should be used to dispose of documents containing identifiable or confidential organisational information. 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 AND DATA PROTECTION

22.1 All information governance incidents, including actual and suspected breaches of confidentiality and data protection, must be recorded on Datix and reported to the Trust Secretary.
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 Serious breaches (those at level two as calculated by the Health and Social Care Information Centre’s online reporting mechanism) will be escalated to commissioners and the Information Commissioner as appropriate, using the relevant reporting mechanism. A summary of level 2 data losses and breaches will also be included in the Trust annual report.

23 **COMPLAINTS ABOUT DATA PROTECTION.**

23.1 The Trust will maintain a procedure for dealing with complaints about the Data Protection 1998 and Freedom of Information Act 2000. The Trust will deal with such complaints within the spirit of the main Complaints Policy and Procedure. However, complainants 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 information securely places the Trust at risk of breaching the Data Protection Act 1998, NHS Caldicott Guidelines and Trust policy. All Trust staff have responsibility for the safety and proper management of the 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
- The Records Management NHS Code of Practice.
- NHS Information Governance - Guidance on Legal and Professional Obligations
- Data Protection Act 1998.
- The common law duty of confidence.
- Computer Misuse Act (1990)
- IT Security Policy
- Information Security and Information Safe Haven Policy
- E-mail and Internet Policy
- Information Governance Framework Policy
- Disciplinary Policy
- Access to Health Records of Inpatients Policy
- Access to Health Records Policy
- Health and Social Care Records Policy and Procedure
- Business and Corporate Records Retention Schedule
- Health Records Retention Schedule
- Mobile Working Policy
- Policy on Social Media
- Confidentiality: NHS Code of Practice
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.
APPENDIX 2– Data Protection Principles

1 First Principle

“Personal data shall be processed fairly and lawfully.”

1.1 The Trust will ensure that the following information is made readily available to people whose data it processes:

- the identity of the data controller
- the identity of any nominated representative for the purposes of the Act
- the purpose(s) for which the data will be processed
- any other information necessary to ensure fairness: such as the likely consequences of processing, and whether they envisage the data being disclosed to a third party.

1.2 The Trust will ensure that processing is carried out only where at least one of the following conditions is met:

- The individual has given his or her consent to the processing.
- The processing is necessary for the performance of a contract with the individual.
- The processing is required under legal obligation.
- The processing is necessary to protect the vital interests of the individual or to carry out public functions.
- The processing is necessary to comply with any legal obligation to which the data controller is subject.
- The processing is necessary for the administration of justice.
- The processing is necessary for Crown, Ministerial or Government functions.
- In the functions of public interest.

1.3 Stricter conditions apply in respect of sensitive personal data. The Trust will process sensitive data only where at least one of the following conditions is met

- Having the explicit consent of the individual
- Being required by law to process the data for employment purposes
- Needing to process the information in order to protect the vital interests of the data subject or another person
- Dealing with the administration of justice or legal proceedings
- For medical purposes
- Where the information has been made public by the individual
- To safeguard the rights and freedoms of the individual, for example to process a subject access request
2 Second Principle

“Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in a manner incompatible with that purpose”

2.1 The Act requires the Trust to notify the purposes for its processing of data to the Information Commissioner. These purposes include:

- Staff Administration
- Accounts & Records
- Health Administration and Services
- Research
- Crime Prevention and Prosecution of Offenders
- Public Health
- Advertising Marketing and Public Relations
- Licensing and Registration
- Accounting & Auditing
- Education
- Handling and Monitoring of Complaints
- Administration of Justice (Mental Health Act Reviews)
- Social Services and Social Work
- Information and Database Administration

2.2 The Information Governance intranet pages will contain an up to date list of these purposes, as notified to the Information Commissioner. The Trust will not collect or otherwise process data for any reasons other than those notified to the Information Commissioner.

2.3 Staff wishing to process data for any reason not already notified to the Information Commissioner must notify the Trust Secretary before doing so.

3 Third Principle

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

3.1 The Trust will collect and use only the minimum amount of information required to fulfil the purpose as notified to the Information Commissioner. Staff will not request additional information unnecessarily.

4 Fourth Principle

“Personal data shall be accurate and where necessary, kept up to date “
4.1 Staff must take reasonable steps to ensure that all data is accurate and up to date.

5 **Fifth Principle**

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes”

5.1 Staff must ensure that personal data is reviewed regularly and retained in accordance with the retention schedules in the Trust’s Records Management Policy and Strategy.

6 **Sixth principle**

“Personal Data shall be processed in accordance with the rights of the data subjects”

6.1 The Trust will respond in a timely manner to subject access requests, or a request to prevent processing. (See section 14 for specific information).

7 **Seventh Principle**

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data “

7.1 Staff must ensure that data is kept securely. This means that the data itself is safe from corruption, deletion, accidental or unauthorised change and physical damage.

8 **Eighth Principle**

“Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensure that an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data “
APPENDIX 3 - Right of Subject Access

1 Requests for access to information

1.1 Any request by an individual (data subject) for access to information held about them must be made in writing (this includes transmission by electronic means).

1.2 The written request must contain sufficient information to enable the Trust to undertake the search required (e.g. Name, Address and Date of Birth). The Trust is not obliged to comply with individuals' requests until the requester has provided adequate information.

1.3 Any request for subject access to a health record should be directed to the Head of Health Records Department at either:

<table>
<thead>
<tr>
<th>Wotton Lawn Hospital</th>
<th>Charlton Lane Centre</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horton Road</td>
<td>Charlton Lane</td>
</tr>
<tr>
<td>Gloucester</td>
<td>Cheltenham</td>
</tr>
<tr>
<td>GL1 3WL</td>
<td>GL53 9DZ</td>
</tr>
</tbody>
</table>

1.4 It is necessary to verify a person’s identity by asking the individual to produce evidence, for example a copy of their driving licence or passport. The Trust does not have to release the information until the request has been received in writing and the required fee has been paid.

2 Fees

2.1 Under the Data Protection Act 1998 (Fees and Miscellaneous Provisions) Regulation 2001 the fees that may be charged to view a health record or be provided with a copy are:

| £10.00  | Maximum fee for copies of health records held on computer only |
| £50.00  | Maximum fee for copies of health records held manually          |
| £50.00  | Maximum fee for copies of health records held in part on computer and in part manually |
| £10.00  | To view the record where no copies required and changes have not been made in the last 40 days |
| No Fee  | To view the record where no copy is required and changes have been made to the record in the last 40 days |

2.2 The maximum fee that can be charged is £50.00. This includes photocopying, postage and packing. The £50.00 will not be charged in all cases but on a recovery basis.
3 Responding to a subject access request

3.1 The Trust must comply with an individual’s request within 40 days of receipt of the written request and the fee. Once this has been received the individual is entitled to be told if any personal data are held about them and, if so:

- to be given a description of the data;
- to be told for what purposes the data are processed and
- to be told the recipients or the classes of recipients to whom the data may have been disclosed.

3.2 They are also entitled;

- to be given a copy of the information with any unintelligible terms explained;
- to be given any information available to the Trust about the source of the data;
- to be given an explanation as to how any automated decisions taken about them have been made

4 Requests from Staff

4.1 The Trust recognises the importance of respecting the privacy of our employees and the need for appropriate safeguards in relation to the collection, storage and other processing of personnel data.

4.2 Staff wanting access to their personal data should make the initial request to their Line Manager, who should contact the Trust Secretary for advice.

4.3 In respect of individuals who no longer work for the Trust, requests should be directed to the Trust Secretary.

5 Exemptions

5.1 There are a number of exemptions from disclosure within the Act, which are for the protection of the data subject and any third parties. Similarly, a third party may request access to personal data that is not their own, such as the law enforcement agencies. There are circumstances within the Act that may permit this to take place.

5.2 In both of these instances, advice must be initially sought from the Trust Secretary before any information is released.

6 Special conditions

6.1 Once the request has been received the Trust must not make any amendments or deletions to the data that would not have otherwise been made. The data must not be tampered with in order to make it acceptable.
6.2 If information is requested that would reveal personal data other than the applicants, the other individual(s) must give consent before it can be released.

6.3 Solicitors and insurance companies may make requests on the behalf of clients. The client involved must sign a written consent form, which needs to be received before any information is released.
APPENDIX 4 – Individual rights under the Data Protection Act

In addition to the right of subject access, the Act provides for the following individual rights:

1 **The right of rectification, blocking, erasure and destruction.**

The Act allows individuals to apply to the Court to order a Data Controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

2 **The right to prevent processing**

An individual can ask a Data Controller to stop or request not to begin processing data relating to them where it is causing, or likely to cause, substantial unwarranted damage or distress to themselves or anyone else. This right is not available in all cases.

3 **The right to prevent processing for direct marketing**

A data subject can ask a data controller to stop or not to begin processing data relating to him for direct marketing purposes. This is an absolute right.

4 **The right to compensation**

A data subject can claim compensation from a data controller for damage or damage and distress caused by a breach of the Data Protection Act. Compensation for distress alone can only be claimed in limited circumstances.

5 **Rights in relation to automated decision-taking**

An individual can ask a data controller to ensure that no decision, which significantly affects them, is based solely on processing his or her personal data by automatic means.