Policy

Data Protection

Key messages

- The holding, using, disposing or sharing of personal identifiable data must comply with the Data Protection Act 2018 and the General Data Protection EU Directive (GDPR)
- Patients must be informed about what we use their information for by issuing them with the 'patient privacy notice – what happens to information held about you'
- There must be a lawful basis in place before personal identifiable data is processed
- The personal identifiable data held by the trust must be accurate and not excessive
- Access to personal identifiable data is on a strict need to know basis
- Patients have the right to access information held about them by contacting the Access to Health Records team
- Staff who are patients of the hospital must not access/view their own information.
- Consent must be given by a statement or a clear affirmative action and must be freely given, specific, informed and unambiguous.

1 Scope

This policy applies to all Trust employees, including:

- staff who hold honorary contracts;
- contractors working on behalf of the Trust;
- the Board of Governors;
- Non Executive Directors.

2 Purpose

- to inform staff of the need to comply with the Data Protection Act 2018 (DPA) and the General Data Protection EU Directive (GDPR);
- to inform staff about what is expected of them and protect them as a user under the Act;
- to protect the Trust as an employer and as a user of personal information.

3 Definitions

Anonymised Information: This is information which does not identify an individual directly; and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of detail that might support identification directly or by association, for e.g. using someone's initials.

Database: collection of personal information that can be processed by automated means e.g. patient records for appointments, patient details for prescribing drugs, patient information used for research or staff records such as training or leavers or starters. Databases that meet this definition could be processed either by using a custom built software system, access program or excel program.

Data controller: This is the person or organisation who either alone or jointly or in common with other persons determines the purpose for which and the manner in which any personal data is processed.

Data processor: Any person or organisation (apart from an employee of the data controller) who processes data on behalf of the data controller.

Data subject: The individual who is the subject of the personal data.

Legitimate Relationships: Controls who has access to a patient's health record; a team of staff or individual health professional can gain access to a patient's record if they have a legitimate relationship with the patient. Access controls to patient's records will be based on legitimate relationships and identified workgroups. Workgroups are groups of staff with identified key activities e.g. doctor or receptionist which determine who can access information and to what level.

Personal data: Personal data that relates to a living individual who can be identified from that data or from that data and other information that is in the possession of or is likely to come in the possession of the data controller (The Trust). Data could include items such as surname, initials, date of birth, address and postcodes, sex, national insurance number, hospital number, forenames, occupation, NHS number, ethnic group, criminal convictions, location data or online identifier. This is not an exhaustive list, personal data can be information that does not include any of these personal details but the individual could be identified from this information and other information in possession of the data controller by association for example medical photograph of a patient with a rare condition.

Processing: In relation to information or data, means obtaining, recording or holding the information or data, carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available or
- alignment, combination, blocking, erasure or destruction of the information or data.

Pseudonymised Information: This is like anonymised information in that it may not be possible for the recipient of the record to identify an individual

for e.g. by use of a unique number in a research project, but the original provider of the information retains the means of identifying the individual. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not. However pseudonymised data may be classed as identifiable data depending on how difficult it is to attribute the pseudonym to a particular individual.

Special categories of personal data: Personal information about an individual that includes religious beliefs, political beliefs, sexual life, membership of a trade union, ethnic background, physical and mental health records and genetic & biometric data are considered sensitive data.
Note: All information regarding health is considered sensitive under the DPA.

4 Introduction

This policy will apply to all personal information for living individuals recorded and held by the Trust.

Deceased information is not subject to Data Protection Act and the General Data Protection EU Directive (GDPR) but still falls under the duty of confidentiality,; please refer to the Confidentiality of Personal Health Policy for further guidance.

The Trust holds and processes information about its employees, patients and other individuals for various purposes.

The Trust is required to comply with the Data Protection Act and the General Data Protection EU Directive (GDPR) when handling personal data in relation to living people.

The Trust is also governed by Human Rights Act 1998, Section 251 and 252 of The National Health Service Act 2006, common law on Confidentiality, Freedom of Information Act 2000, Environmental Information Regulations 2004, Computer Misuse Act 1990, NHS Code of Practice on Confidentiality, NHS Care Records Guarantee, NHS Code of Practice on Information Security, Mental Capacity Act 2005, Caldicott Guidelines, Data Security & Protection Requirements toolkit, NHS Constitution and the Access to Health Records Act.

This policy sets out how the Trust will meet these requirements.

The Data Protection Act 2018 and the General Data Protection EU Directive (GDPR) sets out the data protection principles that organisations need to comply with:

Data Protection Principles
Personal data shall be

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data controllers are responsible for demonstrating compliance with the principles.

Lawful basis for processing

For processing to be lawful under GDPR the Trust needs to identify the lawful basis before we can process data and ensure that this lawful basis is documented.

a) consent of the data subject;
b) processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;
c) processing is necessary for compliance with a legal obligation;
d) processing is necessary to protect the vital interests of a data subject or another person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights of freedoms of the data subject

Conditions for special categories

a) explicit consent of the data subject, unless reliance on consent is prohibited by EU or member state law;

b) processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;
c) processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
d) processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to member or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent;
e) processing relates to personal data manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest on the basis of union or member state law which is proportionate to the aim pursued and which contains appropriate safeguards;
h) processing is necessary for the purposes of preventative or occupational medicine for assessing the working capacity of the employees, medical diagnosis, the provision of health or social care or treatment or management of health care systems and services on the basis of union or member state law or a contract with health professional;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of healthcare and of medical products or medical devices;
j) processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89 (1)

Rights of the data subject

- Right to be informed
- Right of access
- Right to rectification
- Right to erase (right to be forgotten)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

All enactment of rights by individuals on receipt will be complied with within one calendar month.

The Information Commissioners office (ICO) is responsible for ensuring compliance with Data Protection Act 2018 and the General Data Protection EU Directive (GDPR) and providing advice and guidance. The Trust is

required to notify the purposes for which it uses personal identifiable information to the Information Commissioner.

Caldicott Guardian
Health organisations are required to appoint a Caldicott Guardian who is a senior health professional who has the seniority and authority to exercise the necessary influences on policy and strategic planning in relation to data processing and information sharing.

Caldicott principles
The Caldicott principles are concerned with the use and protection of patient identifiable information. All Trust's must abide by these principles:

- justify the purpose – every proposed use or transfer of patient identifiable information within or from another organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian;
- do not use patient identifiable information unless it is absolutely necessary – personal confidential data should not be included unless it is essential for the specified purpose of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose;
- use the minimum necessary – where the use of personal confidential data is considered to be essential, the inclusion of each individual data item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out;
- access to personal information should be restricted on a strict need to know basis – only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes;
- everyone should be aware of their responsibilities – action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect patient confidentiality;
- use of personal information should be lawful – every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements;
- The duty to share information can be as important as the duty to protect patient confidentiality – health and social care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles.

5 Responsibilities

For a full description of information governance responsibilities please refer to the Information Governance policy. This policy outlines specific responsibilities in relation to this policy

Chief Executive: Legally responsible for ensuring complete and continued data notification for the Trust.

Board responsibility: The Executive Director of Improvement and Transformation is responsible for raising issues to the Board of Directors as appropriate.

Information governance lead: Nominated Data Protection Officer for the Trust and designated Caldicott Officer.

- responsible for renewing and maintaining adequate notification;
- to inform the data controller (Trust), data processors (contractors) and employees of their data protection obligations;
- monitor data protection compliance;
- assign responsibilities, awareness-raising and training of staff involved in processing operations;
- undertake internal audits of data protection;
- provide advice on the need and completion of privacy impact assessments;
- co-operate with the ICO and act as contact point for any issues relating to processing;
- undertake or advise on the potential risk of processing activities

They must:

- have access to the organisations data processing personal and operations;
- significant independence in the performance of their roles;
- have a reporting line to the highest management level of the organisation

6 Using, holding, disclosing personal information

The duty to inform

The Trust is required to inform individuals why we hold their information, for what purposes we use their information and with whom we may share their information with.

Privacy notices are made available to staff and patients, via the Trust website and through other communication channels. Topic specific privacy notices will be made available to groups of individuals as required.

The Patient privacy notice 'What happens to information held about you' is available on the Trust's website and can be printed on request. Posters are placed in clinical areas to inform patients of the privacy notice.

Supplementary information should be available to patients if information is used for any other purposes that are not included in this privacy notice.

In order to ensure that patients are informed effectively, staff should:

- check that the privacy notice has been read and understood;
- inform patients when information is recorded or health records accessed;

- inform patients when information will be shared with others;
- check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;
- check that patients have no concerns or queries about how their information is disclosed and used;
- answer any queries personally or direct the patient to others who can answer their questions;
- respect the rights of patients.

Information for staff about what the Trust does with staff personal information is contained within the Protecting and keeping confidential employee data available on the intranet and in the staff privacy notice.

Adequate, relevant and not excessive
The level of personal information held should be adequate, relevant and not excessive, always use the minimum amount of identifiable data and justify the use of that information, where possible personal information should be anonymised, as this can be used with few constraints.

Accurate and up to date
All personal information must be accurate and up to date. This is to ensure that we provide the best possible patient care and that we run an efficient business.

Patients details must be checked at every visit by asking open questions for example: What is your address? Ensure that any changes are updated as soon as possible.

Staff must inform their line manager of any changes to their personal details as soon as possible.

Protecting personal information
Keeping all personal information secure is vital. Opportunity puts temptation in an individuals way so all Trust staff must adhere to the security measures to protect personal information and the safe haven procedures when sharing personal information, please refer to the Information Governance Policy.

Access to personal information
All personal data must be treated as confidential and must not be disclosed to anyone who is not authorised to receive it. For further guidance on the sharing of personal information please refer to the Confidentiality of Personal Health Information policy and procedure or the Protecting and keeping confidential employee data .

Access
Staff must only have access to personal data on a strict need to know basis for the purpose of the role that they are employed to do, for e.g.

- for health care, where the employee has a 'legitimate relationship' with a patient, this includes both health care professionals and administrators;

- for personnel issues where the employee is the line manager of another employee or is authorised to access personnel files;
- where the employee is authorised to access personal data/create records in specific circumstances e.g.
  - Legal services in medico legal cases
  - Dealing with complaints
  - Clinical auditors
  - Clinical coders
  - Researchers
  - Risk managers/ representatives
  - Investigating officers
  - Finance staff
  - Information management team

Staff who are patients of the hospital must not view their own information. If they would like access to their health records please refer to section 11.

Staff must not look up friends or family member details unless they are involved in their healthcare.

Managers are not allowed to access medical information about their staff and their staff's families.

From time to time staff will see people that they know who are themselves attending the hospital. It is important that staff deal with such situations in a tactful and professional manner. The reason for attendance remains confidential to the patients unless they wish to divulge such information willingly to a staff member.

Data on all electronic systems must be accessed by staff by using their own log on and personal password and should not be shared; appropriate access controls must be in place.

For further guidance please refer to the Guidance for staff: accessing patient records in Epic

In-appropriate access

If a patient or staff member has concerns that a patient health record may have been accessed in-appropriately they must contact the information governance team, the information governance team will undertake an investigation into the enquiry/concerns.

All enquiries will be investigated following the Methodology for in-appropriate access. If it is found that a member of staff(s) may have accessed a patient(s) record in-appropriately then the case will be referred to HR to be investigated under the Trust disciplinary process.

Investigations are time bound; if in-appropriate access is more than 6 months earlier, a discussion will take place with HR/staff(s) line manager to

decide if a HR investigation is appropriate. Informal action will still be undertaken with the staff(s) for cases not investigated by HR.

Audit reports
The Electronic Patient Record logs all access and changes to the patient health record, including whether a record has just been viewed.
A patient is entitled to request a copy of this audit report. This will include a list of staff who have accessed their record, including job title and department.

Patients should contact the information governance team if they would like an audit report of who has accessed their health record. For further information please refer to section 11, subject access.

Audits
The information governance team will undertake proactive audits to monitor staff access to the electronic patient record, for e.g. staff accessing patient records with the same surname, questionable access audit and staff who have accessed an excessive number of patient records.

Processing/using personal information
For processing to be lawful under Data Protection Act 2018 the Trust needs to identify the lawful basis before we can process data and that this lawful basis is documented, please refer above. Personal data must only be processed for the purpose that they were gathered and must not be used for any other purposes without a legal basis or ensuring the individual has been informed of the processing.

- Staff are not allowed to process private data on Trust premises using Trust equipment;
- processing private personal data, whilst undertaking a course of study, is at the manager's discretion. The manager should notify the Data Protection Officer in writing with the employee's name, reason for using the Trust equipment and the data being processed for example identifiable;

Private data – refers to any data that is not Trust data, required for as part of the Trust business and activities, for e.g. data for the running of a separate business or data relating to a staff members home life.

Right to object
Individuals have the right to block or suppress processing of personal data. When processing is restricted we are permitted to store the personal data but no longer process it. We are also able to retain sufficient data to ensure the restriction is protected in the future.

Patients have the right to object to the use of their personal information. If this would compromise the provision of healthcare, then the risks must be explained to the patient and a compromise reached if possible.

All decisions regarding patients' wishes must be recorded in Epic as an alert. Requests from patients should be forwarded to the information governance team.

Right to erasure (right to be forgotten)
Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This is not an absolute right. The right to be forgotten only applies when:

- personal data is no longer necessary in relation to the purpose that they were originally collected/processed;
- the individual withdraws consent;
- the individual objects to processing and there is no overriding legitimate interest to continue processing;
- the personal data was unlawfully processed
- the personal data has to be erased in order to comply with legal obligation;
- the personal data is processed in relation to the offer of information society services to a child (this refers to online services provided for children)

Requests can be refused

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); for archiving purposes in the public interest, scientific research, historical research or statistical purposes
- to exercise the defence of legal claims
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

Please refer all requests to the Trust data protection officer.

Right to rectification
Individuals may apply for their information to be rectified if information relating to them is inaccurate or incomplete.

Requests must be dealt with within one calendar month.

If requests cannot be enacted the individual must be informed of the decision and their right to complain to the information commissioner's office.

Please refer all requests to the Trust data protection officer.

Right to portability
Individuals have the right to receive personal data about them in a 'commonly used and machine readable format, this right is only available where the processing is based on consent or and the processing is automated.

Requests from individuals should be referred to the Trust Data Protection Officer.

Retention and disposal of personal information
Personal information should not be retained for longer than necessary. The Department of Health sets out retention periods for a variety of documents, all information should be retained to comply with the retention and destruction schedules, for further guidance please refer to the Records, Retention and Destruction Policy and Procedure.

All personal/ confidential information should be destroyed securely, for further guidance please refer to the Information Governance Policy and the Waste Disposal Policy.

Education and training
Use of patient identifiable data in presentations/publications/training material must either be anonymised or patient explicit consent must be sought.

As a teaching hospital we support students through their clinical placement, we also support the education and learning of all our staff throughout their careers. As a result of this education programme staff will view and access patient identifiable data held in our Electronic Patient Record (EPR) or through clinical consultations directly with patients. Explicit consent is not required from the patient for access to their information in our EPR. Patients must be consulted for a student/member of staff to sit in on a clinical consultation.
Patients are informed that their information may be accessed for education purposes in our privacy notice 'what happens to information held about you'. Patients do have the right to object, if they have objected to their information being used for this purpose an alert will be placed on their record 'information excluding education'.

Education portfolios should only include anonymised patient records unless explicit consent has been obtained from the patient.

External assessors/trainers should only be given access to patient identifiable information if it is justifiable and the patient has given explicit consent.

7 Consent

Where we rely on Consent for the processing of personal data –
Consent must be given by a statement or a clear affirmative action and must be freely given, specific, informed and unambiguous. Consent must be a positive opt in.

It must be easy to withdraw consent and we must inform individuals when obtaining their consent how to do this.

We must be able to demonstrate that we hold consent from the individual. Consent must be regularly reviewed.

Further guidance for staff on asking for consent from individuals to process their personal data is available from the Trust Data Protection Officer.

8 Information Mapping – inbound/outbound flows of information

Information flows should be identified for the processing and sharing of all personal information. This is to ensure that we keep personal information secure, know for what purpose we are using personal information, and comply with the safe haven procedures and the Caldicott principles.

All departments will be required to maintain an Information Mapping Log; this must be reviewed on a yearly basis. For further guidance please contact the information governance team.

9 Notification/ Registration

The Trust must notify the Information Commissioner of:

- a description of the personal data being processed and the categories of the data subjects to which they relate;
- a description of the purposes of processing;
- a description of any recipients to whom the data controller intends or may disclose the data to;
- the name or description of any countries or territories outside the European Economic Area to which the data controller transfers or intends to transfer data;
- a description of the security measures taken to protect personal data.

Data must only be used for purposes declared in the Trust's notification and must not be used for other non-registered purposes.

Information governance must be made aware of all new Databases. The Trust's Database Registration Form must be completed and sent to the information governance team. The purpose for the use of the data will be checked against the Trust's Data Protection Notification so that any new

processing can be added to the Trust's notification. The system will be added to the Trust's Information Asset Register, held by Information Governance.

Registration forms are available on Database Registration Form.

10 Privacy by design/Privacy Impact Assessments

New systems/processes should not be purchased or implemented until they have been approved by Information Governance. For further guidance please refer to the Information Governance Policy.

11 Subject access

All individuals, or in certain circumstances someone acting on their behalf, can request a copy of their personal data held by the Trust. An individual who makes a subject access request is entitled to:

- be told by the Trust whether any personal data is held about them, and
- be supplied with a copy of the information that forms any such personal data.

The Trust must respond to requests within a calendar month. Requests will be processed free of charge. A reasonable fee can be charged when a request is 'manifestly unfounded or excessive' particularly if repetitive or for repeat copies. The fee must be based on the administrative cost of providing the information.

Requests from patients

- patients can approach a clinician who is currently treating them to view information held about them relating to the current treatment that they are undergoing;
- alternatively they can put in a written request to obtain access to any information held about them. All written requests for personal information should be date stamped with the date of receipt and forwarded to the Access to Health Records Officer, box 82;
- for audit reports of who has accessed their health record please contact the information governance team at gdpr.enquiries@addenbrookes.nhs.uk
- for further guidance please refer to the Subject access policy.

Requests from staff and other individuals

- they can put in a written request to the data protection officer to gain access to any information held about them. All written requests for personal information should be date stamped with the date of receipt and forwarded to the Information Governance Team, box 153;
- for further guidance please refer to the Subject access policy

12 Contract clauses

All contractors employed by the Trust will be required to comply with the Trust's Data Protection, Confidentiality and Security requirements.

Contracts must include appropriate clauses to comply with Information Governance.

All data processors:

- need a contract in place with the correct clauses in place as outlined in Data Protection Act 2018;
- processors must provide sufficient guarantees;
- must follow instructions of the data controller;
- if they employ a sub-contractor then the data processor must have a contract in place with them.

For further guidance please refer to the Information Governance Policy

13 Automated decision making

Currently there is no automated decision making taking place.

Any intended automated decision making must be discussed with the Trust Data Protection Officer before it is put in place.

14 NHS Care Records Guarantee

The NHS Care Records Guarantee sets out the 12 commitment to patients with regard to the NHS Care Record and local patient records; this includes how we share information and with whom, patients right of access to information held about them, that staff are trained in their responsibilities, that we will adhere to the NHS Code of Practice on Confidentiality and that we will have audit processes in place to know who has accessed patient records.
The Trust is committed to complying with all 12 commitments.

15 Training and advice

All staff will received information governance training as outlined in the Information Governance & Information Security policy

16 Breaches, incidents, disciplinary, compensation, complaints process

It is each member of staff's responsibility to maintain personal data in line with this policy and ensure it is secure. A breach of the Data Protection Act could result in the Trust receiving an enforcement notice, a fine or being audited by the Information Commissioners Office. Staff who commit a deliberate or careless breach of the Act will face disciplinary proceedings which could result in the loss of employment.

Further guidance is available in the Information Governance Incident Investigation Procedure.

17 Accountability and governance

All organisations are expected to put in place comprehensive and proportionate governance measures such as:

- implementing technical and organisational measures that ensure and demonstrate we comply with the GDPR principles;
- maintain documentation on processing activities;
- appoint a data protection officer;
- implement measures that meet principles of data privacy by design and data protection by default
- undertake privacy impact assessments;
- adhere to approved codes;
- adhere to retention schedules;
- maintain information mapping flows

18 Request for information from the data protection officer

In undertaking their duties the Trust Data Protection Officer or their representative may require any staff member to provide information. Requests must be dealt with within the time frame outlined in the enquiry. Extensions can be granted where required by a staff member but will be limited to the statutory timeframes set out in the regulation/Act.
The Data Protection Officer has the right to request and be provided with information that they require to undertake their duties. Information will be kept secure and confidential, where information is required for release as part of an investigation/compliant or subject access request staff will be informed of this disclosure, concerns raised by staff will be taken into consideration but ultimately the Trust will have to comply with the regulation/Act.

19 Complaints or concerns

If any individual has any concerns or complaints in how their personal data is being handled by the Trust please refer the enquiry or the individual to the Trust Data Protection Officer.

20 Advice and guidance

If any member of staff requires any guidance or advice about data protection or GDPR or the content of this policy please contact the Trust Data Protection Officer.

21 Monitoring compliance with and the effectiveness of this document

Key standards to be monitored:

- the holding, using, sharing and disposing of personal identifiable information complies with the requirements of the Data Protection Act

The standards will be monitored by the information governance team by:

- audits will be undertaken as per the information governance monitoring and assurance spread-sheet;
- monitoring information risk assessments and incidents, the Information Governance Lead are notified of all incidents and risk assessments relating to information governance. The IGSG receives a monthly report on information risk assessments and incidents raised. The IGSG is responsible for ensuring that any actions are implemented by the IG team or department.

22 References

Data Protection Act 2018 and the General Data Protection EU Directive (GDPR
NHS Code of Confidentiality
Data security and protection requirements toolkit

23 Associated documents

Policies and Procedures
Confidentiality of Personal Health Information policy
Records: preservation, retention and destruction policy and procedure
Records Management policy and procedure
Freedom of Information policy and procedure
Home Working Policy
Waste Management Policy
Information Governance & Information Security Policy
Information Governance Incident and Investigation Procedure
Subject access policy
Methodology for investigating in-appropriate access to Epic

Equality and diversity statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

Disclaimer

It is **your** responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

The table below will be completed by the Trust Documents Team:

Approval:	Information security, governance & programme board		
Owning department:	Information Governance		
Author(s):	Information Governance Lead		
File name:	Data Protection Policy V13		
Supersedes:	12		
Version number:	13	Review date:	
Local reference:		Media ID:	328

Reviewed: 01 July 2021