# DATA PROTECTION POLICY

<table>
<thead>
<tr>
<th>Version:</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified by:</td>
<td>Trust Executive Committee</td>
</tr>
<tr>
<td>Approved by responsible committee(s):</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Name/title of originator/policy author(s):</td>
<td>Paul Kenny, IG Manager</td>
</tr>
<tr>
<td>Lead Executive(s):</td>
<td>Peter Davies, Director of Corporate Services</td>
</tr>
<tr>
<td>Date issued:</td>
<td>13 March 2019</td>
</tr>
<tr>
<td>Review date:</td>
<td>March 2021</td>
</tr>
<tr>
<td>Target audience:</td>
<td>All staff</td>
</tr>
</tbody>
</table>
CONTENTS

1. INTRODUCTION ........................................................................................................ 3
2. Scope ...................................................................................................................... 3
   The Policy applies to: .............................................................................................. 4
3. Definitions ............................................................................................................... 4
4. Duties & Responsibilities ..................................................................................... 9
5. THE POLICY .......................................................................................................... 12
6. Related Legislation and Guidance ...................................................................... 31
7. Appendix 1 .......................................................................................................... 33
8. Appendix 2: ......................................................................................................... 35
9. Appendix 3: .......................................................................................................... 36
10. Appendix 4 ........................................................................................................ 37
11. Appendix 5 ........................................................................................................ 38
12. Appendix 6 ........................................................................................................ 42
13. EQUALITY IMPACT ASSESSMENT FORM ...................................................... 44
1. INTRODUCTION

Epsom and St Helier University Hospitals NHS Trust has a legal obligation to comply with all appropriate legislation in respect of obtaining and disclosing personal information in accordance with Data Protection Act 2018 (DPA).

The Data protection act applies to all information either manual or electronic that identifies a living individual (a natural person). In order to comply with the DPA information must be processed in accordance with the six principles of the DPA.

Processing refers to the way information is held, obtained, recorded, used and shared.

Accountability is central to the Data Protection Act 2018, Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

The Trust also has a duty to comply with guidance issued by the Department of Health, NHS Digital the NHS Executive, advisory groups to the NHS as well as guidance issued by professional bodies. These guidelines should not conflict with this policy or legislative requirements.

This policy details how the Trust will meet its legal obligations and NHS requirements regarding the confidentiality and security of personal information.

The Caldicott principles (appendix 1) provide guidance on the use of and or transfer of personal information and the key recommendation out of the 16 in the Caldicott 2 report was that: “a senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information”. (Recommendation 3)

The nominated individual is known as the Caldicott Guardian.

The National Data Guardian (NDG) standards (July 2016) (appendix 2) set out 10 actions to be undertaken to assist in protecting information from loss, damage or inappropriate use.

2. SCOPE

This Policy applies to all permanent, temporary or contracted staff employed by Epsom and St Helier University Hospitals NHS Trust, including non-executive directors, students and volunteers. It includes all data which is about a living individual and is held in any format including, but not exclusively, written and electronic.

This Data Protection policy sets out how the Trust will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act
2018 that is the key piece of legislation covering security and confidentiality of personal information.

The Data Protection Act 2018 applies to all records, both in electronic and manual formats that identifies, or could identify, an individual that are held and processed by the Epsom and St Helier University Hospitals NHS Trust.

As above the Act applies to the processing of most forms of personal data including, but not exclusively, data held in the following which is not an exhaustive list:

- Databases
- Electronic filing systems (such as the H:\ and G:\ drives)
- Audit trails
- Emails
- Excel Spreadsheets
- Word Documents
- Paper Files / filing systems
- CCTV
- Audio Recordings
- Photographs
- X-ray, CT, MRI
- Portable Media, memory sticks, disks, phones, cameras
- Payment systems

The Trust as a “Data Controller” is responsible for all records detailed above and has submitted a notification to the Information Commissioner – Registration No. Z6690929

The Policy applies to:

- All information used by the Trust;
- All information systems managed by or for the Trust;
- Any individual using information ‘owned’ by the Trust;
- Any individual requiring access to information ‘owned’ by the Trust;
- Any individual working on behalf of the Trust, or anyone who accesses Trust premises and information which is owned or managed by the Trust.

3. DEFINITIONS

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

- Organisation, adaptation, 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
- Blocking, deletion/erasure or destruction of the information or data.
The Trust advocates the method of remembering the definition of “Processing” by using the acronym HORUS – Holding, Obtaining, Recording, Using and Sharing.

**Accessible Public Record** - Records kept by a public body such as the Trust and covered by the Public Records Act 1958.

**Anonymised Data** - Data from which the identity of an individual cannot be determined. Anonymisation requires the removal of name, address, full post code and any other detail or combination or details that might support identification.

**Biometric** - Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (finger prints).

**Caldicott Committee** - The name of the Committee formed to review the use of patient identifiable information in the NHS. Named after its chair person, Dame Fiona Caldicott.

**Caldicott Principles** - A set of principles to control the use or flow of patient-identifiable information

**CCTV** - Closed Circuit Television

**Code of Practice** - A set of documented procedures used by public bodies to ensure they comply with legislation. For example, the NHS code of confidentiality.

**Common Law** - A law which is determined by decisions made by the courts and can therefore change over time. A law set by precedents.

**Confidentiality** - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

**Confidential Information** - Confidential information could include, without limitation details of:
- Business Contacts, associates, list of suppliers and details of contract with them.
- Identities of patients
- Expenditure levels and Trust specific pricing policies
- Proposal plans or specification for the development of existing services and of new services
- Details of employees and officers of the Trust and of the remuneration and other benefits paid to them
- Presentations, tenders, projects, joint ventures, mergers and developments contemplates, offered or undertaken by the Trust

**Consent** - Consent is the fact that permission has been given. A person who consents to something is, in effect, giving permission for that thing to happen.
**Data** - A collection of facts from which conclusions may be drawn; "statistical data".

**Data Controller** - This is the authority which defines the purposes for which personal data is processed. The Trust is a data controller.

**Data Processor** - Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data Protection Act 2018** - UK wide legislation that governs the use of personal information. Its purpose is to protect the right of the individual. The Act laid down six data protection principles.

**Data Protection Officer** - The person within an organisation, in this case the Trust, who is responsible for compliance with the Data Protection Act.

**Data Protection Principles** - The set of standards for good practice in information processing as defined in the Data Protection Act 2018. The Act laid down six data protection principles.

**Data Subject** - An individual whose personal data is held by an organisation. For example, a data subject can be a patient but also a member of staff who's personal information is held by the Trust.

**Destruction** - Process of eliminating or deleting records, beyond any possible reconstruction.

**Disclosure** - The release of personally identifiable data to a third party.

**DPA** - Data Protection Act 2018

**Explicit or Express Consent** - This means the individual has articulated agreement either orally or in writing. Both terms are used to describe circumstances where a clear and voluntary preference or choice, is given. It must be given freely in circumstances where the available options and the consequences have been made clear.

**Fair Processing** - The first principle of the 2018 Data Protection Act is that personal data must be processed fairly and lawfully. In order to achieve this, individuals must be made aware of, and consent to, the ways in which information about them may be collected and used.

**Filing System** - Means any structured set of personal data which are accessible accordingly to specific criteria, whether centralised, decentralised on functional or geographical basis.

**Genetic Data** - Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the
physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

**Health Record**

“health record” means a record which—
(a) consists of data concerning health, and
(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;

This includes mental or physical health. The definition also applies to Occupational Health Records.

Thus, with the exception of anonymised information, most if not all NHS information concerning patients, whether held electronically or on paper, will fall within the scope of the Act.

**Identifiable Data** - Data items that can be used to identify an individual, also referred to as personal data or personal information.

**Information Sharing Protocol (ISP)** - Documented rules and procedures for the disclosure and use of patient information between two or more organisations or agencies.

**Manual Data/ Records** - Information that is not processed by means of equipment.

**Medical Purposes** - As defined in the Data Protection Act 2018, means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

**NHS Code of Confidentiality** - A guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients’ consent to the use of their health records.

**Personal Data** -
“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**Personal Data Breach** - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Profiling - Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Processing - Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymised Information - Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Public Interest - Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.

Research
Research – the attempt to derive generalisable new knowledge including studies which aim to generate hypotheses as well as studies that aim to test them.
https://www.hra.nhs.uk/planning-and-improving-research/research-planning/access-study-support-advice-services/

Restriction of Processing - The marking of stored personal data with the aim of limiting their processing in the future.

Special Category Data - Personal data consisting of a person’s:
- Racial or ethnic origin,
- Political opinions,
- Religious beliefs or beliefs of a similar nature,
- Membership of a trade union,
- Physical or mental health or condition,
- Sexual life

Data relating to criminal offences and convictions
Which are addressed separately under the Law Enforcement Directive of the Data Protection Act 2018 (as criminal law lies outside the EU's legislative competence)

Special Purposes - A term used in the Data Protection Act 2018. It refers to data used for the purposes of journalism, artistic or literary purposes.
4. DUTIES & RESPONSIBILITIES

The policy applies to all Trust employees, volunteers and all partners, suppliers and service providers to the Trust. It is compulsory that all those who work for the Trust whether as an employee, volunteer, contractor or a supplier comply with this policy, related policies and sub policies and the standards, guidelines and procedures that are derived from them.

The Chief Executive has overall responsibility for the Data Protection Policy within the Epsom and St Helier University Hospitals NHS Trust.

**Caldicott Guardian and Chief Clinical Information Officer**

The Caldicott Guardian is responsible for safeguarding and governing the uses of patient information within the Trust, acting as the ‘conscience’ of our organisation. The Caldicott Guardian should actively support work to facilitate and enable information sharing and advice on options for lawful and ethical processing of information as required.

The Caldicott Guardian (and others) will use the Caldicott principles to help determine when person confidential information should be shared. See appendix 1 for the principles.

In their role as Chief Clinical Information officer the post holder will provide digital health and care leadership to the Trust, leading the successful adoption of digital technologies across the Trust supporting clinicians and leaders to attain the best possible impact that modern technology can have.

**The Senior Information Risk Owner (SIRO)**

The SIRO is responsible for ownership of the Trust’s Information Risks, to act as an advocate for information risk on the Board. The Trust’s SIRO is the Director of Corporate Services. The SIRO is a signatory to Trust DPIA’s.

**Deputy Director of ICT**

The Deputy Director of ICT will oversee the implementation of the National Data Guardians security standards across the Trust (see Appendix 2) and the day to day running if the ICT department of systems.

**Information Governance Manager | DPO**

The Information Governance Manager is the Trusts designated Data Protection Officer.

The Trust Data Protection Officer’s role includes:

- Maintaining the Trust Notification (Maintains the Trust's entry in
Inform and advise the Trust's awareness of the Act, including the development of policies, procedures and guidance for individuals to support their understanding and compliance with this policy

Monitor compliance through the auditing of staff compliance with the Act and related policies

Facilitate staff annual IG training

Acting as point of expertise for any data protection issues which may arise within the Trust and providing advice for staff when completing a Data Protection Impact Assessment

Support the Trust's Caldicott Guardian and SIRO

Be the point of contact for the ICO and ensure full co-operation with the ICO when required

Notifying Data Protection serious breaches within 72 hours through the Data Security and Protection Toolkit or its' successor

The Infrastructure Manager
Will maintain a list of all systems, IAO’s and IAA’s as well as other documentation required for the management of Trust systems and completion of the NHS Digital Data Security and Protection Toolkit.
Will ensure systems are updated and patched in accordance with policy and NHS guidance.
Ensures appropriate data backups are regularly taken.
Ensures suitable and sufficient anti-malware systems are in place and kept updated on Trust systems.
Will ensure suitable firewalls are in place.
Provides regular reports to the information governance committee as required by the information governance committee.

Customer Support Manager / Registration Authority (RA) Manager
The customer support manager working with the infrastructure manager ensures that software on end user devices is supported and maintained correctly and that hardware provided meets Trust specification.

Ensures documentation required for the management of Trust systems and completion of the NHS Digital Data Security and Protection Toolkit.

The customer support manager also fulfils the role of RA manager. The RA manager carries out identity checks of prospective smartcard users and assigns an appropriate access profile to the health professional's role as approved by the Trust.

Provides guidance to smart card users
Carries out RA security spot checks.
Provides regular reports to the information governance committee as required by the information governance committee.
Divisional Clinical Directors / Divisional General Managers (IAO) will ensure that:

- Information Asset Owners will be supported by Information Asset Administrators, but the overall responsibility for the management of the Trust information assets sit with the Information Asset Owners.
- All databases and their respective owners are notified to the Infrastructure manager
- Information Asset Owners (IAO’s) / Information Asset Administrators (IAA’s) / are appointed for all departmental databases/information systems and their details notified in writing to the Information Governance Manager | DPO via the Information Security Officer
- Appropriate local systems are in place regarding manual files held in the department that contain personal details (typically patient or staff records)
- Information is used for the purposes declared and that it is maintained and disposed of in accordance with Trust policies
- staff undertake appropriate training
- All staff are aware of data protection through training including induction
- All staff are made aware at Induction of their personal responsibilities in respect of confidential and personal data
- systems are in place to check the accuracy of personal data held in their departments about staff or patients
- The legal basis for processing for personal information the IAO is responsible for is documented and kept up to date.
  - Provides regular reports to the information governance committee as required by the information governance committee.
  - ensure expert advice is sought regarding Data Protection issues
  - Ensure annual flow mapping is completed ensuring each instance of processing is identified and documented.

Application Owners / Systems Administrators / Managers (IAA) will:

- Confirm in writing their acceptance of the role of IAO / IAA
- It is the responsibility of the Trust’s delegated Information Asset Owners to ensure that all information assets are documented and kept appropriately secure, in line with the Data Protection Act Principles and are not kept for longer than necessary.
- ensure that information is processed in accordance with the Trust ICO Notification
- system and user manuals are available for each system
- Users are set up on the system on a need to know basis with access restricted to their role
- Expert advice is sought regarding Data Protection issues
- disclosures of information are checked against the Notification
- Unusual requests for disclosure are scrutinised
- make their staff aware of their responsibilities regarding security, data
All staff will:

- Comply with Terms and Conditions of Employment
- Comply with the requirements of the Data Protection Act 2018
- Comply with the Trust’s Data Protection and Confidentiality Policy, including any procedures and guidelines which may be issued from time to time.
- Ensure that any information about individuals is collected in a timely and accurate fashion.
- That they comply with Trust requirements in terms of storage of person specific information, including security provision
- To be responsible for ensuring that they attend or complete online Information Governance.
- Ensure the correct data protection legislation is referred to in documentation to aid transparency.
- When completing incident reports provide sufficient information including contact information to allow the incident to be followed up in a timely manner.
- Comply with Trust Policies

Distribution

This policy will be made available on the Trust’s intranet.

5. THE POLICY

Data Protection

The Trust has a legal obligation to comply with all appropriate legislation in respect of Data, Information and ICT Security. It also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, other advisory groups to the NHS and guidance issued by professional bodies.

Personal information may be collected from patients, employees, volunteers and suppliers (past, present and future) and others the Trust interacts with for various purposes including for example the provision of healthcare services, the running of payroll and to enable communications.

All legislation relevant to an individual’s right of confidence and the ways in which that can be achieved and maintained are paramount to the Trust. Legislation applies to roles that are reliant upon computer systems such as: patient administration/payment, purchasing, invoicing and treatment planning. Legislation also regulates the use of manual records relating to patients, staff and others whose
information may be held within the Trust. It also extends to information held in other relevant filling systems.

Penalties could be imposed upon the Trust, and/or employees for non-compliance with relevant legislation and NHS guidance. The Information Commissioner has powers to fine organisations up to €20,000,000 (approximately £17,000,000) or 4% of total annual worldwide turnover for breaches of the DPA 2018.

If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is 10 million Euros (or equivalent in sterling) or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

The Data Protection Act 2018, Human Rights Act 1998 and the Freedom of Information Act 2000 are interlinked. They are intended to maintain a fair balance between the rights and interests of individuals, in particular the freedom to process information on the one hand, and the rights of privacy on the other.

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. A brief summary of the DPA2018 and associated legislation and guidelines are detailed in Appendix 1.

There are six principles of good practice within the Data Protection Act 2018. These are normally referred to as the ‘data protection principles’.

In the following it must be noted that the GDPR is implemented through the DPA 2018.

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(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 (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes 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 the Legislation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(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 (‘integrity and confidentiality’).

GDPR Article 5 (2) adds - The Data Controller shall be responsible for, and be able to demonstrate compliance with, paragraph (a) above (‘accountability’).

Access to rooms and offices where computers / smart cards are present or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card.

In mixed (other organisations or teams) office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

INDIVIDUALS RIGHTS

In the following it must be noted that the GDPR is implemented through the DPA 2018.

The data protection act 2018 affords the following rights to individuals:

- **Transparent information**, communication and modalities for the exercise of the rights of the data subject (this is included in our Privacy Notice on the Trust web site). **(Articles 12-14)**

- Information to be provided where personal data are collected from the data subject (the Privacy Notice). **(Article 15)**

- Information to be provided where personal data have not been obtained from the data subject.

- **Rights of access by the data subject** (Subject Access Requests)
  - Right to rectification. **(Article 16)**
    - See Trust web site and below

- **Right to erasure** (right to be forgotten) (n.b. does not apply to health records which are covered by the Public Records Act 1950). **(Article 17)**

  A data subject has the right to request that the Trust erases their personal data where one of the following conditions applies.
• The personal data is no longer necessary in relation to the purposes for which they were collected.
• The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
• The personal data has been unlawfully processed.

Where the Trust receives a request of this nature it will be passed to the Information Governance for consideration in line with the Records Management Code of Practice for Health and Social Care 2016 (retention schedule), who will then provide a response to the data subject.

• **Right to restriction of processing (Article 18)**
  The data subject has the right to request that the Trust restricts processing their data when:
  • accuracy of their personal data is contested
  • processing is unlawful
  • the Trust no longer needs the personal data for the purposes of processing
  • the data subject has objected to the processing of their personal data, pending verification on whether the legitimate grounds of the controller overrides those of the data subject.

  This right applies to factual information only, not to opinions or a diagnosis that the patient disagrees with or which turns out to be wrong.

  An individual who believes that an organisation has recorded inaccurate personal information about them and it is likely to cause damage or distress is entitled to send a written notice to the Trust requesting that processing of their data stop, or does not begin. The individual must be able to show that he/she has suffered or would suffer substantial and unwarranted damage or distress if the processing goes ahead.

  The Trust does not have to comply where it believes the processing is so important it must go ahead even though it causes damage or distress. The individual can apply to court to overrule Trust decision.

• **Right to data portability. (Article 20)**

  This means that data subjects have the right to receive personal data about them in a ‘….. commonly used and machine readable format’ when the processing is carried out by automated means. The Trust’s legal basis for processing an individual’s personal data is not reliant on the explicit consent of the data subject, which means that this right is not applicable to the Trust’s processing of personal data.
• **Right to object. (Article 21)**

The data subject has the right to object to how the Trust is processing their data. For individuals to exercise this right, they must submit their request to the Information Governance Department.

The right to object does not apply where the individual has consented, the processing is necessary to comply with a legal obligation or to protect the vital interests of the individual.

• **Rights in relation to automated decision making and profiling (Article 22)**

This right does not apply to all circumstances but, where it does apply, it effectively provides data subjects with safeguarding against the risk that a potentially damaging decision is taken solely using or supported by automated means, without human intervention.

The data subject has the right not to be subjected to a decision based solely on automated processing, including profiling. This right does not apply to the Trust as the Trust does not undertake any automated decision making or profiling.

**NHS Opt-out**

- The Trust acknowledges the review undertaken in 2016 by the NHS and Social Care National Data Guardian. The review not only agreed that the NHS and Social Care need to process patient information on a wider scale to help improve the care and treatment delivered, but also agreed that there were circumstances when patients can choose to opt out with how the NHS uses their information.


The Trust will ensure that where patients have exercised their rights to opt-out of their information being used for secondary purposes, this will be recorded on the Trust’s system and respected.

**Consent**

The DPA 2018 (incorporating the GDPR) sets a high standard for consent, but the biggest change from previous legislation is what this means in practice for consent mechanisms. There needs to be clear and more granular opt-in methods, good records of consent, and simple easy-to-access ways for people to withdraw their consent.
Consent is to be treated as an ongoing and actively managed choice and not simply a one off indication of consent.

The definition of consent in Article 4(11) of the GDPR as incorporated into the DPA 2018:

“any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”

Key elements of the consent definition – it must be freely given, specific, informed, and there must be an indication signifying agreement. The DPA 2018 is clear that the indication must be unambiguous and involve a clear affirmative action.

Several provisions on consent contain more detailed requirements. In particular, Article 7 sets out various conditions for consent, with specific provisions on keeping records of consent, clarity and prominence of consent requests, the right to withdraw consent, and avoiding making consent a condition of a contract (provision of service). Recitals 32, 42 and 43 also give more specific guidance on the various elements of the definition.

This means there is a strong emphasis in the DPA 2018 (which incorporate the GDPR) on individuals having clear distinct ('granular') choices upfront and ongoing control over their consent.

If consent is withdrawn the processing of information obtained under consent must be halted.

An example may be the withdrawal of consent to receive a “newsletter”.

For the purposes of “Direct Care” which includes administration of care and clinical audit, the Trust relies on its public function under the Health and Social Care Act and that the processing is for Medical Purposes, rather than consent.

See the legal basis for processing below.

Common Law of Confidentiality

The Common Law of Confidentiality is created by judicial precedent (case law also known as tort) rather than Act of Parliament, that ‘information confided should not be used or disclosed further, except as originally understood by the confider or with their subsequent permission’.

Generally, if a data subject’s information is disclosed in circumstances where it is expected that a duty of confidence applies, it should not normally be disclosed further without that data subject’s consent.

In the provision of health and social care this duty applies very strongly in the service user / professional relationship.
There are instances where the Duty of Confidentiality can be overridden e.g. in public interest, national security and statutory requirements. When the Trust is requested to set aside the Common Law Duty of Confidentiality, this decision is not taken likely, and the Caldicott Guardian has the responsibility of acting in the best interests of the data subject (patient/individual) in deciding whether the Trust would set aside the Common Law Duty of Confidence.

The Duty of Confidentiality is further enforced through staff codes of practice of their respective professions (e.g., NMC, GMC, CIPFA, CIMA) and by virtue of their contract with the Trust. These codes of practice should not conflict with this policy or legislative requirements.

In death our Duty of Confidentiality remains and requests in relation to information about deceased persons will fall under the Access to Health Records Act 1990.

**Data Privacy Impact Assessments (DPIA)**

A Data Privacy Impact Assessment (DPIA) is “a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. DPIAs help identify privacy risks, foresee problems and bring forward solutions.”

The DPIA will help to ensure that potential problems are identified at an early stage in design of the project.

Reasons for undertaking a DPIA include:

- To identify privacy risks to individuals.
- To identify privacy and Data Protection compliance liabilities for the Trust.
- To protect the reputation of the Trust.
- To instil public trust and confidence in our processes and information handling. (DPIA’s are normally published on the Trust web site).
- To avoid expensive, inadequate “bolt-on” solutions.
- To inform the communications strategy regarding the process.
- To reduce the likelihood of regulatory action including fines against the Trust.

It is essential that all new information systems / processes go through the Information Governance Manager IDPO and are subject to a DPIA completed by the relevant IAO. Changes to existing information systems/ processes should also undergo a DPIA.

Information systems, that is systems that process person identifiable information, may include but are not limited to:

- Computerised systems,
- PC’s,
- Tablets,
- PDAs,
Servers,
Spreadsheets,
Databases,
Analysers,
Scanners,
Imaging systems,
Medical Equipment,
Diagnostic equipment,
RFID Tagging and Tracking,
Paper based filing systems.

The Information Governance Manager | Data protection Officer should be consulted if any assistance is required to complete a DPIA.

See the Information Governance page on the intranet for a template DPIA. The Information Commissioners website may provide further guidance.

**Accuracy of Data**

As mentioned previously personal information held by the Trust must be accurate and up-to-date.

Staff are responsible for:

Checking that any patient, staff or other individual’s information they handle is accurate and up to date. At every point of contact with the individual, staff should ask for confirmation on their current demographic and contact information that the Trust is holding, e.g. address.

Reporting inaccurate data. Staff members with sufficient rights to amend data must do so as soon as they are made aware of the inaccuracies. Otherwise staff must bring the discrepancy to the attention of the system administrator or line manager.

The DPIA process:
Information Sharing Agreements

The Trust and health and social care providers across South West London have adopted a two tier approach to Information Sharing Agreements. Tier one is the overarching Information Sharing Agreement which sets out the framework for information sharing between organisations. This encompasses the legislation, guidance and best practice but does not include the actual sharing of information.
Tier two is the Purpose Specific Information Sharing Agreements (PSISAs) these cover in detail the sharing of information for specific purposes between the named organisations. The PSISA covers the reason for the sharing, the cohort of patients, what information will be shared, how it will be shared and how often, updates, retention, actions at the end of the agreement and accuracy as well as the legal basis for sharing. In some cases the PSISA will also incorporate a Data Privacy Impact Assessment (DPIA) instead of the DPIA being a separate document.

The Information Governance Manager | DPO will assist in the completion of PSISAs.

Please note that where a PSISA is not used information sharing between organisations MUST be covered by Contract or Service Level Agreement with similar provisions to the PSISA. A PSISA may also be used in addition to the Contract or Service Level Agreement.

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) 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.

Data Processing Agreement

Where the Trust engages with another company to undertake services, and the company will be processing the Trust’s personal or special category data, the Trust will ensure that it has put in place a data processing agreement with the company/supplier.

The Information commissioner’s office states:
“Under the Data Protection Act 1998 (“the 1998 Act”), a controller that employed a third party to process personal data on its behalf (a “processor”) could demonstrate its compliance with the security principle by having a contract in place with the processor.

Typically, this contract would have required the processor to only act upon the controller’s instructions and to take appropriate measures to keep the personal data secure.

Under the DPA 2018, there is a separate obligation to have a contract. Also, contract requirements are more wide-ranging and are no longer confined to just ensuring the security of personal data. They aim to ensure that the processing of personal data, by a processor, will comply with all the GDPR’s requirements and protect the rights of data subjects. The GDPR sets out specific terms that must be included in the contract, as a minimum.

The contract must state details of the processing, and must set out the obligations and rights of both the controller and the processor. It must also include the standards the processor has to meet when processing personal data.

This is a significant change to what the 1998 Act required. However, in practice, existing contracts may have already included some of the new requirements for commercial reasons or as good practice under the 1998 Act.

The GDPR also allows the contract to include standard contractual clauses issued by the European Commission or a supervisory authority, such as the ICO. Again this is a significant change in the law but, initially at least, it should make little practical difference as standard clauses are not yet available.

In the future, processors may be able to demonstrate they provide ‘sufficient guarantees’ to process personal data in line with the GDPR by adhering to an approved code of conduct or certification scheme. No such codes or schemes have been approved so far so, initially at least; this should make little practical difference.

The main difference is that processors now have direct GDPR responsibilities and obligations, outside the terms of the contract. Processors can be held directly responsible for non-compliance with their data protection obligations. They may be subject to administrative fines or other sanctions and liable to pay compensation to data subjects.

**Legal Basis for processing**

It is the responsibility of information asset owners (IAO’s) to maintain a record of the legal basis for processing of the personal data they are responsible for.

All health and social care providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to both the Common Law Duty of Confidence
and the Data Protection Legislation and, for the purposes of direct care the Trust relies on its public function under the Health and Social Care Act that the processing is for Medical Purposes, rather than rely on consent.

For common law purposes, sharing information for direct care is on the basis of implied consent, which may cover administrative purposes where the patient has been informed or it is otherwise within their reasonable expectation. This approach is valid for confidentiality purposes (Common Law Duty of Confidence), provided the patient is appropriately informed, or the proposed activity is obvious or can be reasonably expected.

Guidance on recording the legal basis can be found on the Information Governance page of the intranet.

The Trust’s legal basis for processing personal data for delivery of direct care and for the providers’ administrative purposes, under GDPR Article 6, is:

\[ 6(1)(e) \text{ ‘...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...’} \]

For personal data concerning health and special category (sensitive) personal data; the most appropriate Article 9 condition for direct care or administrative purposes is:

\[ 9(2)(h) \text{ ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’} \]

The Information Governance Manager | DPO may be consulted regarding the completion of the record which should be returned to the Information Governance Manager | DPO

See appendix 5 - Conditions for Processing Special Categories of Personal Data (Sensitive data)

These conditions will also be the most appropriate for the local administrative purposes such as:
- waiting list management
- performance against national targets
- activity monitoring
- local clinical audit
- production of datasets to submit for commissioning purposes and national collections.

These conditions will also apply where an organisation participates in activities with a statutory basis such as responding to a public health emergency.
The lawful basis and conditions for processing data other than for direct care is as follows:

<table>
<thead>
<tr>
<th>Type of data</th>
<th>Personal Data – Article 6</th>
<th>Special Category Data – Article 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff</td>
<td>6(1)(e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority…’</td>
<td>9(2)(b) ‘…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of… social protection law in so far as it is authorised by Union or Member State law…’</td>
</tr>
<tr>
<td>Safeguarding children and vulnerable adults</td>
<td>6(1)(e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority…’</td>
<td>9(2)(b) ‘…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of… social protection law in so far as it is authorised by Union or Member State law…’</td>
</tr>
<tr>
<td>Research (Note: unless Information shared with consent or with s251 support)</td>
<td>6(1)(e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority…’</td>
<td>9(2)(j) ‘…scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate… and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject…’</td>
</tr>
</tbody>
</table>

**Notification of Data Security and Protection Incidents**

Incidents must be reported on the Trusts Datix incident reporting system and will be graded against the NHS Digital framework as set out in the “Guide to the notification of Data Security and Protection Incidents” as updated from time to time. External reporting of incidents to NHS Digital and the Information Commissioner will be via the Data Security and Protection Toolkit. The Information Governance Manager | DPO or other individual as delegated by the Senior Information Risk Owner will complete notifications. As set out in the DPA 2018 reports of incidents or suspected incidents that reach the reporting criteria will be reported within 72 consecutive hours of the Trust becoming aware of the incident or potential incident. To be clear Bank holidays and Weekends are included in the 72 hour time frame.

It is vital that divisional quality managers review and action incidents in a timely manner.
Subject Access Requests

Individuals both patients and staff have the right to access their personal data and supplementary information, subject to certain restrictions.

This right allows individuals to be aware of and verify the lawfulness of the processing you are carrying out.

Patients will be made aware of their right of access to their records (by making a subject access request).

Details of how to make a subject access request can be found on the Trust web site including information on charges if there are any.

Handling Subject Access Requests made by, or on behalf of, a current or past patient will generally be dealt with by the Subject Access Request (SAR) team which is part of the Medical Records Department (or those authorised; see Appendix 4A). In some circumstances the Caldicott Guardian, SIRO or the Information Governance Manager | DPO may also be involved.

The Trust Caldicott Guardian will oversee disclosures of patient information with particular attention being paid to extraordinary disclosures (those which are not routine). This role of Caldicott Guardian will be carried out in accordance with the guidance in HSC 1999/012 Caldicott Guardians.

For requests for patient information between NHS organisations and/or Social Care organisations for continuing patient care the Department which is dealing with the patient should provide the minimum information necessary to fulfil the request to the requesting organisation by secure means. The Medical Records Subject Access Team must be consulted if in doubt.

Staff SARS will be managed and provided by the Human Resources department see below.

Patient Information

There are specific requirements highlighted within the Caldicott recommendations (Caldicott principles appendix 1) that apply to patient identifiable information. Most of these are also requirements of compliance with the Data Protection legislation. Specifically they relate to security, confidentiality and fairly obtaining information as well as ensuring all disclosures are valid and authorised.

All patient information, whether manually or automatically held, will be kept secure both when not being used for a patient care or related purpose and when in use for patient care and related use.

The guidance relating to good handling practice for records is contained within the Information Governance Alliance Records Management Code of Practice for Health
and Social Care 2016. This is also incorporated into the Trust Health Records Policy which can be found on the Trust intranet.

See appendix 3 - the six principles of data protection and appendix 2 the NDG Data Security Standards.

Patients will be made aware of how their data will be processed and how they can object to that processing. This may be by the use of information posters in patient waiting areas, statements in patient handbooks/on survey forms, the Trust web site where the Trusts privacy notice) can be found and verbally by those health care professionals providing care and treatment.

**National Data Opt-Out Programme**

The national data opt-out is a national service provided by NHS Digital that allows patients to opt out of their confidential patient information being used for research and planning.

When processing patient data for research and planning purposes the national data opt-out must be consulted.

By 2020 all health and care organisations are required to be compliant with the national data opt-out policy, where confidential patient information is used for research and planning purposes.

See the section below: Related Legislation and Guidance

---

**Disclosure of Personal Patient Information – further considerations**

There are Acts of Parliament that govern the disclosure / sharing of personal patient information – some make it a legal requirement to disclose and others that state that information cannot be disclosed.
These Acts are detailed below:

**Legislation to restrict disclosure of personal identifiable information**

- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

**Legislation requiring disclosure of personal identifiable information**

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

Legislation to restrict disclosure of personal identifiable information:
- Venereal Diseases Act 1917 and Venereal Disease Regulations of 1974 & 1992

**Staff Information**

Any member of staff / temporary staff, volunteer or apprentice - current, past or potential (applicant), who wishes to have a copy of their employment information under the subject access provision of the DPA2018 should contact in the first instance, the Head of Operational HR or the Information Governance Manager| DPO. A Staff Subject Access procedure and Application pack is available on the Trust intranet.

**Contracts of Employment**

Staff contracts of employment are produced and monitored by the Trust Human Resources department. All contracts of employment must include data protection and general confidentiality clauses. Agency and contract staff and volunteers are subject to the same rules.

All Trust employees will be made aware of their responsibilities in connection with the Acts mentioned in this Policy through their Statement of Terms and Conditions,
through Mandatory Training and targeted training sessions carried out by Application Managers and/or other trainers/specialists.

**Training**

All new staff must complete Information Governance / Security training as part of their induction.

All staff, Volunteers, Bank staff and Non-Executive directors must complete Information Governance / Security training annually (within the financial year 1\textsuperscript{st} April to the 31\textsuperscript{st} March the following year).

Some staff, for example health records staff, SIRO, Caldicott guardian may be required to complete additional training as mandated by the Information Governance Committee.

**Disciplinary**

A breach of the DPA2018 requirements or those of other legislation may result in a member of staff facing disciplinary action. A copy of the Disciplinary Procedures is available from the Human Resources Department or from the intranet.

Specific use of information in contravention of Trust Policy could lead to the individual being prosecuted under the Data Protection Act 2018 and other legislation. Data subjects may also take action against individuals who have breached legislation in regard to their personal information.

**Complaints**

Individuals also have a right to complain if they believe the Trust is not complying with the requirements of the Data Protection Legislation.

Complaints which may be received because of a breach, or suspected breach, of the Data Protection Legislation will be dealt with under the Trust Complaints Policy.

**Information Commissioners Office (ICO)**

Failure to comply with the principles and relevant legislation will leave the Trust, and/or employees, open to substantial monetary fines and reputational damage. The Information Commissioner has powers to fine data controllers and processors for serious data breaches, up to £17 million or 4\% of global turnover for the most serious breaches.
Change Control Board (CCB)

New information systems (including those that are in existence but new to the Trust) or changes to existing information systems and processes related to confidential information must be approved by the CCB before they go ahead.

The Trust ICT change control board meets regularly to review changes to software, hardware system and processes.

The procurement team will not purchase information systems or changes to systems without CCB approval.

The CCB process can be seen in appendix 6 the Trust intranet should be consulted for the latest version.

RESEARCH

All research studies must have confirmation of capacity and capability from the Trust Research & Development (R&D) department in writing prior to commencing their research.

R&D Confirmation of Capacity and Capability will be issued only after the research study has been reviewed by the R&D Capacity and Capability Committee and the R&D Department has been provided, by the Study Sponsor, with confirmation of NHS Health Research Authority (HRA) approval, and a favourable opinion from the Research Ethics Committee and MHRA approval (where applicable). Other approvals maybe required.

The Research and Development department will determine if Researchers who are not Trust staff are required to have an honorary contract or letter of access (LoA) prior to starting their research project.

It is a Trust requirement that research participants (usually patients) are informed how their information is to be used before they are asked to provide it (code of practice on confidential information: 2014 https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf ) or as soon as possible.


All researchers should ensure that they are aware of the requirements of the Data Protection Act (2018) and other relevant data protection legislation as well as the
confidentiality measures agreed in their ethics application as well as the Caldicott requirements.

It is a Trust requirement that the correct legislation and guidance is referred to in all research documentation.

See Appendix 5 for the legal basis for processing in regard to research.

**Confidential Waste**

Unwanted printouts and other documents containing person-identifiable or confidential information must be put into a confidential waste bin / console.

Confidential waste consoles / bins will be kept locked and kept securely, where wheeled bins are used these must be chained to a wall or other suitable point of attachment to prevent theft of the bin.

The Estates and Facilities team must be contacted regarding the secure disposal of bulk material and the ICT Help Desk must be consulted regarding the secure disposal of storage media such as CD /DVD, Hard disk, computers, printers. This is not an exhaustive list. See the ICT electronic and media disposal policy for further guidance.

**HOW THE POLICY WILL BE MONITORED, AUDITED AND REVIEWED**

Compliance with this policy is to be monitored at local level and by the Information Governance Committee which will receive regular reports from Information Asset Owners on the systems they are responsible for that process / store personal information (timing and content as determined by the chair of the information governance committee) from information asset owners at least once every financial year (April 1st to March 31st the following year).

This policy will be the subject of a regular review by the Information Governance Committee which will take place at not less than at two yearly intervals. Earlier review may be triggered in response to feedback from training, regulatory changes or in response to critical incidents and regulatory changes.

**Relevant Policies / Procedures and guidance relating to Data Protection**

Related policies

Information Governance Policy
Information Security Policy
6. RELATED LEGISLATION AND GUIDANCE

This is not a definitive list:

Data Protection Act 2018 (and subsequent Special Information Notices)
Freedom of Information Act 2000

General Data Protection Regulation 2016/679

Human Rights Act 1998

Access to Health records act 1990
Common Law of Confidentiality
Computer Misuse Act 1990

Copyright, designs and patents Act 1988 (as amended by the
Copyright (Computer Programs) Regulations 1992

Electronic Communications Act 2000

Regulations 2000)
Crime and Disorder Act 1998

IMG:E5498 Ensuring Security and Confidentiality in NHS Organisations
HSG (96)18 The Protection & Use of Patient Information
HSC 1999/012 Caldicott Guardians
HSC 2002/003 Implementing the Caldicott Standard into Social Care

Gateway Ref 6295 and 10678 Records Management: NHS Code of Practice

techniques – Code of Practice for Information security Management

Codes of practice for handling information in health and care

Records Management Code of Practice for Health and Social Care 2016
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/n/b/records-management-cop-hsc-2016.pdf
https://digital.nhs.uk/binaries/content/assets/legacy/excel/o/o/rmcop-retention-schedules.xls

Code of practice on confidential information
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf

HSCIC Guide to Confidentiality 2013
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/0/d/hscic-guide-to-confidentiality_2013.pdf
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/0/n/confidentiality-guide-2013-references.pdf

Confidentiality

Information security management NHS code of practice

NHS Information Governance - Guidance on Legal and Professional Obligations

Code of conduct for data-driven health and care technology - updated Feb 2019
National Data Opt-Out Programme


7. **APPENDIX 1**

The Caldicott principles

**The Seven Caldicott Principles**

1. Justify the purpose(s) of using confidential information.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Access should be on a strict need to know basis.
5. Everyone must understand his or her responsibilities.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.

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

The original Caldicott Report, established six principles for NHS bodies (and parties contracting with such bodies) to adhere to in order to protect patient information and confidentiality.

It is acknowledged that NHS staff have become more reluctant to share information given the potential sanctions in doing so inappropriately.

Accordingly, the government commissioned Dame Fiona Caldicott to conduct a further Information Governance Review (the “Review”) which was published at the end of April 2013.
“The duty to share information can be as important as the duty to protect patient confidentiality”. The Review highlights that for health professionals to act in a patient’s best interest, they need to have all the available information about the patient to do so. However, it is acknowledged that current information governance provisions (or at least the interpretation of them) have led to information not being shared when it should be. Accordingly, Recommendation 2 of the Review specifically states that:

“for the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Further, the Review also recognises that there are certain situations when sharing of personal information is not just preferable, but vital. An example given of this is within public health medicine in order to identify people at risk during an outbreak of an infectious disease, or to carry out health improvement and research exercises.
8. APPENDIX 2:

NDG DATA SECURITY STANDARDS

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

2. All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

8. No unsupported operating systems, software or internet browsers are used within the IT estate.

9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.
9. **APPENDIX 3:**

**THE 6 PRINCIPLES OF DATA PROTECTION**

1) Processes lawfully, fairly and in a transparent manner

2) Collected for specified, explicit and legitimate purposes

3) Adequate, relevant and limited to what is necessary

4) Accurate and where necessary kept up to date

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and

6) Processed in a manner that ensures appropriate security of the personal data.
10. APPENDIX 4

The following staff or their teams may handle the processing of Subject Access Requests and must have procedures to support their processes:

- Medical Records Manager
- Director of Workforce
- Radiology Services Manager (for x-rays and other scan images)
- Legal / Claims Manager / Complaints
- Information Governance Manager | DPO
- Others at the request of the Information Governance Manager | DPO

Please note that for inpatients it is recommended that they only apply for Subject Access Request once they have been discharged.

If a competent inpatient is adamant about seeing their records, the Consultant in charge of the patient’s care MUST give authorisation.

The Consultant will ensure that the exemptions in the legislation are applied, if relevant – i.e that the patient (or person seeing the records) should not come to mental or physical harm as a consequence of seeing the records and that third party information provided in confidence is not disclosed.

If a relative or friend of an inpatient demands to see the patients’ record, the patient, if competent, MUST be consulted first without the undue influence of the relative or friend. In addition the Consultant, as well as checking for the exemptions above must also take care that if there is information in the record that the patient does not want disclosed this is also obeyed.

In either case above if the Consultant deems that exemptions apply or if the patient is not competent, then the formal Subject Access Process should be followed. The Subject access team based in the Medical Records Department should be consulted regarding any queries in the first instance.

SEE THE HEALTH RECORDS POLICY FOR DETAILED GUIDANCE
11. **APPENDIX 5**

**Conditions for Processing Special Categories of Personal Data (Sensitive data)**

Special Categories (Sensitive) Personal Data is defined as

- Racial or ethnic origin
- Political opinion
- Religious or philosophical belief
- Trade Union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

**GDPR ARTICLE 9- Conditions relevant for processing of special categories of personal data**

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the
personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever 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 shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 4.5.2016 L’119/38 Official Journal of the European Union EN

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Note: for processing patient health information the Trust is relying on ...

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

Article 6

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if the organisation is a public authority processing data to perform your official tasks.)

In Summary:

For Direct Care

The Trust’s legal basis for processing personal data for delivery of direct care and for the providers’ administrative purposes, under GDPR Article 6, is:

6(1) (e) ‘…necessary for the performance of a task carried out in the public interest or in the exercise of official authority….’

For personal data concerning health and special category (sensitive) personal data; the most appropriate Article 9 condition for direct care or administrative purposes is:

9(2) (h) ‘…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems….’

These conditions will also be the most appropriate for the local administrative purposes such as:
These conditions will also apply where an organisation participates in activities with a statutory basis such as responding to a public health emergency.

The lawful basis and conditions for processing data other than for direct care is as follows:

<table>
<thead>
<tr>
<th>Type of data</th>
<th>Personal Data – Article 6</th>
<th>Special Category Data – Article 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff</td>
<td>6(1) (e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’</td>
<td>9(2)(b) ‘...is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of... social protection law in so far as it is authorised by Union or Member State law...’</td>
</tr>
<tr>
<td>Safeguarding children and vulnerable adults</td>
<td>6(1) (e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’</td>
<td>9(2)(b) ‘...is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of... social protection law in so far as it is authorised by Union or Member State law...’</td>
</tr>
<tr>
<td>Research (Note: unless information shared with consent or with s251 support)</td>
<td>6(1) (e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’</td>
<td>9(2)(j) ‘...scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate... and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject...’</td>
</tr>
</tbody>
</table>
12. APPENDIX 6

Change Control Process

Refer to the intranet for the latest version
The CCB will require sight of completed documents such as but not limited to:

DPIA
Legal basis for processing
Flow mapping
SOP
Information sharing agreement
Data processing agreement
Contract
13. **EQUALITY IMPACT ASSESSMENT FORM**

In order to carry out an effective impact assessment it is important to examine all available data and research so that any adverse impact on disability can be properly assessed.

<table>
<thead>
<tr>
<th>1. Name of function, strategy, project or policy</th>
<th>Data Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Name, job title, department, and the telephone number of staff completing the assessment form</td>
<td>Paul Kenny, Information Governance Manager DPO Tel 721 2244</td>
</tr>
<tr>
<td>3. What is the main purpose and outcomes of the function, strategy, project or policy.</td>
<td>Epsom and St. Helier University Hospitals NHS Trust has a legal obligation to comply with all appropriate legislation in respect of person confidential data.</td>
</tr>
<tr>
<td>4. List the main activities of the function, project/policy (for strategies list the main policy areas)</td>
<td>This Data Protection policy sets out how the Trust will meet its obligations in regard to data protection.</td>
</tr>
<tr>
<td>5. Who would benefit from the strategy/project/policy</td>
<td>All those whose personal data is held by the trust.</td>
</tr>
<tr>
<td>6. Is it relevant to:</td>
<td>Yes</td>
</tr>
<tr>
<td>- Race Relations Act</td>
<td>In that person confidential information must be protected appropriately.</td>
</tr>
<tr>
<td>- Sex Discrimination Act</td>
<td></td>
</tr>
<tr>
<td>- Disability Discrimination Act</td>
<td></td>
</tr>
<tr>
<td>- Employment Equality Regulations</td>
<td></td>
</tr>
<tr>
<td>- Religion or Belief</td>
<td></td>
</tr>
<tr>
<td>- Sexual Orientation</td>
<td></td>
</tr>
<tr>
<td>- Age</td>
<td></td>
</tr>
<tr>
<td>7. Do you think that the function/strategy/project/policy could have a negative or positive impact on:</td>
<td>Overall positive affect as the policy sets out to protect person confidential information.</td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Disability</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td></td>
</tr>
<tr>
<td>Religion</td>
<td></td>
</tr>
<tr>
<td>Sexual Orientation</td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
</tr>
<tr>
<td>8. How could you minimise or improve any negative impact?</td>
<td>N/A</td>
</tr>
<tr>
<td>Impact? Explain how.</td>
<td>Review by the information governance committee. Review by the interim head of performance and information.</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9. What consultation with relevant users on this project has taken place.</td>
<td>N/A</td>
</tr>
<tr>
<td>10. If there are gaps in your consultation and research, are there any experts/relevant groups that can be contacted to get further views or evidence on the issues. Please list them and explain how you will obtain their views.</td>
<td>N/A</td>
</tr>
<tr>
<td>11 a) Have you involved your staff in taking forward this impact assessment? 11 b) How have you involved the staff</td>
<td>N/A</td>
</tr>
<tr>
<td>12. In the light of all the information detailed in this form what practical actions would you take to reduce or remove any adverse/negative impact.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

To be signed by the Manager completing this form.

Signed................................................................. Date: