Committed To Excellence | Working Together | Facing The Future

Frimley Health NHS Foundation Trust

Trust Policy

Data Protection and Confidentiality Policy

Key Points

- The General Data Protection Regulation (GDPR) came into force on 25th May 2018, and is the biggest change to data protection legislation in 20 years, fundamentally changing the way organisations must handle and look after people's information.
- The Data Protection Act 2018 is the UK law mirroring the GDPR for when the UK leaves the European Union.
- All information held in either manual or electronic format that identifies an individual must be processed (held, obtained, recorded, used and shared) in accordance with the six principles of the Data Protection Act 2018
- All staff have a legal obligation to keep information secure and to protect confidential information from disclosure under the Common Law Duty of Confidentiality
- Individuals are entitled to ask the Trust for copies of information that is held about them
- All staff must receive Information Governance Training on an annual basis to ensure they are up to date on Trust policies and procedures

Version:	2.0
Role of Policy Lead(s):	Head of Information Governance
Role of Executive Lead:	Director of Finance (SIRO)
Date Approved by Executive Lead:	July 2018
Name of Professional Approving Group:	Information Governance Committee
Date Approved by Professional Approving Group:	June 2018
Date Approved by Policy Review Group:	June 2018
Date Ratified by Hospital Executive Board:	July 2018
Date Issued:	July 2018
Review Date:	June 2021
Target Audience:	All Staff
Key Words & Phrases:	Data Protection Act, Confidentiality, Caldicott Guardian

Version Control Sheet

Version	Date	Policy Lead(s)	Status	Comment
0.1	01/11/16	Head of Information Governance	Draft	Transferred to new format
1.0	07/02/17	Policy Officer	Final	Ratified at HEB
1.1	02/05/18	Head of Information Governance	Draft	Updated to reflect GDPR and Data Protection Act 2018
1.2	06/06/18	Information Governance Administrator	Draft	Numbering and Legislation date update
2.0	10/07/2018	Policy Officer	Final	Ratified at Top Team

Document Location

Document Type	Location
Electronic	Policy Hub

Related Documents

Document Type	Document Name
Trust Policy	Information Governance Policy

Contents

	Page No
1. Introduction	4
2. Scope of the Policy	4
3. Definitions	5
4. Purpose of the Policy	5
5. The Policy	6
6. Duties / Organisational Structure	15
7. Raising Awareness / Implementation / Training	17
8. Monitoring Compliance of Policy	17
9. Equality Impact Assessment	17
10. References	17
Appendix A: Data Protection Act 2018 Principles	18
Caldicott Principles	

1. INTRODUCTION

1.1 Frimley Health NHS Foundation Trust ("the Trust") holds and processes information about its employees, patients and other individuals for various purposes (e.g., the effective provision of healthcare services; and/or to operate the payroll and to enable correspondence and communications).

1.2 To comply with the Data Protection Act 2018 ("the Act"), all information either manual or electronic that identifies a living individual must be processed (held, obtained, recorded, used and shared) in accordance with the six principles of the Data Protection Act 2018.

1.3 All NHS employees are bound by the Common Law Duty of Confidentiality, placing a legal duty on all staff working for the Trust to keep all information provided to the Trust and themselves as employees of the Trust by its patients completely confidential. This legal obligation is further enforced through the codes of practice of staff's respective professions and by virtue of their contract with the Trust.

1.4 Professional bodies (e.g., NMC, GMC, CIPFA, CIMA) often release guidelines and advice for their own disciplines. These guidelines should not conflict with this policy or legislative requirements.

1.5 Frimley Health NHS Foundation Trust is committed to the provision of a service that is fair, accessible and meets the needs of all individuals.

2. SCOPE OF THE POLICY

2.1 The Department of Health Confidentiality Code of Practice 2003 outlines the working practices that an NHS Trust must adopt in order to deliver patient confidentiality that is required by law, ethics and policy, with an objective of continuous improvement.

2.2 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. This relates to all information held in the Trust relating to all its patients, staff and any other individual who comes into contact with the Trust.

2.3 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 Frimley Health NHS Foundation Trust.

2.4 The Trust as a "Data Controller" is responsible for all records detailed above and has submitted a notification to the Information Commissioner – Registration No. Z5031452.

2.5 The Policy will apply 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

3.1 "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.

3.2 The Trust advocates the method of remembering the definition of "Processing" by using the acronym HORUS – Holding, Obtaining, Recording, Using and Sharing.

3.3 A glossary of Terms, which covers all aspects of Information Governance, is included as an annexe to the Trust's Information Governance Policy. This glossary refers to terms which the user may find in any of the Information Governance documentation. The list is dynamic and may be updated at any time to reflect changes in guidance or legislation.

4. PURPOSE OF THE POLICY

4.1 This Data Protection and Confidentiality Policy outlines the legal framework that governs the confidentiality of all information held by the Trust by detailing the legal obligations under the Data Protection Act 2018 which underpins the NHS Confidentiality Code of Practice 2003 that all staff must comply with.

4.2 The Trust is continually changing its processes and systems to further improve the Trust's compliance with the Data Protection Act 2018 and staff are responsible for ensuring they keep up to date with Trust policies, procedures and guidance.

4.3 Whilst working for the Trust, staff will have access to information about patients and/or about the Trust. Staff may find this information out as part of their work or see, hear or read something while on Trust premises.

4.4 All staff have a legal obligation to ensure that any confidential information they come into contact with is kept secure and confidential at all times. Where a member of staff receives a request for information relating to an individual, staff must ensure that any disclosure of confidential information is fully justified and in compliance with the Data Protection Act 2018 or Common Law Duty of Confidentiality.

4.5 Where staff are unsure of whether to disclose the requested information or not, staff must refuse to disclose the information and seek advice from their immediate

supervisor; or, if this is not possible, seek advice from, or forward the person making the request to the Trust's Head of Information Governance or Caldicott Guardian or the Information Governance Department.

5. THE POLICY

5.1 LEGAL OBLIGATIONS

5.1.1 Caldicott Guidelines

In 1997 the Caldicott Committee Report found that confidentiality and security compliance was patchy across the NHS. In response to this patchy compliance across the NHS, the Caldicott Committee developed 6 principles which staff must apply when using patient information.

5.1.2 The 2013 Information Governance Review, amended the 6 Caldicott principles to include a seventh Caldicott principle:

1. Justify the purpose(s);
2. Don't use personal confidential data unless it is absolutely necessary;
3. Use the minimum necessary personal confidential data;
4. Access to person confidential data should be on a strict need-to-know basis;
5. Everyone with access to personal confidential data should be aware of their responsibility;
6. Comply with the law;
7. The duty to share information can be as important as the duty to protect patient confidentiality.

5.1.3 A detailed explanation of the 7 Caldicott principles can be found at Appendix A.

5.2 NHS Confidentiality Code of Practice

5.2.1 The Department of Health Confidentiality Code of Practice published in 2003 states its implementation will enable an NHS organisation to achieve a confidential service in which all patient information is processed fairly, lawfully and as transparently as possible.

5.2.2 The Department of Health Confidential model has 4 main elements:

PROTECT – look after patient's information

5.2.3 In order to provide a confidential service, the Trust needs to ensure that it protects patient information at all times, so only staff who have a need to access the confidential information can do so.

5.2.4 Staff should check that any callers, by telephone or in person, are correctly identified (please refer to IG Guidance on the Intranet).

5.2.5 There could be a significant risk of harm to a patient through impersonation by those seeking information improperly.

5.2.6 Staff should share the minimum information necessary to provide safe care or to satisfy other legitimate purposes, bearing in mind that missing information can harm patient care.

5.2.7 A patient's confidentiality must be respected in response to enquiries from external individuals or organisations (e.g., media, police, and insurance companies). In these circumstances express consent must be obtained from the patient and/or proper (legal) authority demonstrated before any disclosure is made.

5.2.8 Staff must not use any of the Trust's IT systems to make an unauthorised disclosure or copy of confidential information belonging to the Trust.

INFORM – ensure that patients are aware of how their information is used

5.2.9 The Trust must inform patients of the intended use of their information, giving them the choice to give or withhold their consent and protect their identifiable information from unwarranted disclosure.

PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways.

5.2.10 Patients have different needs and values – this must be reflected in the way that they are treated, both in terms of their medical condition and the handling of their personal information. Staff must:

- Seek the patient's consent prior to using their information in ways that do not directly contribute, or support the delivery of their care;
- Respect a patient's decisions to restrict the disclosure or use of their information, other than where exceptional circumstances apply;
- Communicate effectively with patients to ensure they understand the implications if they choose to agree or restrict the disclosure of their information.

IMPROVE – always look for better ways to protect, inform and provide choice

5.2.11 The Trust accepts that technology changes, therefore the Trust will continually review its processes to ensure that the 4 elements of the Department of Health Confidentiality is protecting patient information to the highest level at all times.

5.3 Common Law Duty of Confidentiality

5.3.1 A duty of confidentiality arises when one person discloses information to another (e.g., patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. This is a legal obligation that is derived from case law, built up over many years.

5.3.2 This Common Law Duty of Confidentiality places an obligation on all individuals working in and for the Trust to ensure that all confidential information which they come into contact with is kept securely and remains confidential.

5.3.3 Whilst the Data Protection Act 2018 only covers living individuals' information, the Common Law Duty of Confidentiality ensures that a patient's right to confidentiality continues after their death.

5.4 General Data Protection Regulations (GDPR)

5.4.1 GDPR adds in new concepts of Accountability and Demonstrability for the processing of personal data on organisations, as well as increasing the rights of an individual to how organisations process their personal data.

5.5 UK Data Protection Act 2018

5.5.1 The Data Protection Act 1998 has been repealed by the Data Protection Act 2018, and mirrors the GDPR and will remain in force, as GDPR no longer applies once the UK has exited the EU. The purpose of the Act is to enhance, protect the rights and privacy of individuals, and to ensure that data about them cannot be processed without their knowledge or consent wherever possible.

5.5.2 The Act covers personal data relating to living individuals.

5.5.3 The Act stipulates that any organisation processing personal data must comply with 6 principles of good practice. The legally enforceable principles are:

1. Processing of personal data must be lawful and fair,
2. Processing of personal data must be specified, explicit and legitimate and not processed in a manner which is incompatible with the purpose for which it was collected,
3. Processing of personal data must be adequate, relevant and not excessive,
4. Processing must be accurate and kept up to date,
5. Processing must not be kept for no longer than necessary for the purpose for which it is processed,
6. Processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

5.5.4 An explanation of the 6 Data Protection Act Principles can be found in Appendix A.

5.6 Regulatory Authority - Information Commissioner

5.6.1 Under the Data Protection Act 1998, there was a legal obligation on organisations to register with the Information Commissioners office, therefore and the Trust will continue to keep this registration up to date, details of this registration can be found on the Information Commissioner's website.

5.6.2 Under Article 30 of the GDPR, the Trust is required to keep a record of processing activities and will review this register on an annual basis, to ensure all processing of personal data is recorded and kept accurate and up to date.

5.7 Legal Basis for Processing Personal / Special category Data

5.7.1 "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;
- Blocking, deletion/erasure or destruction of the information or data, also
- The Trust advocates the method of remembering the definition of "Processing" by using the acronym HORUS – Holding, Obtaining, Recording, Using and Sharing.
- The Trust has identified its legal basis for processing personal data under the GDPR / Data Protection Act 2018 as;

Type of data	Patients/Customers	Staff
Personal Data (Article 6)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller (Article 6(e)).	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract of employment (Article 6(b)).
Special Category Data (Article 9)	We will use your information to provide preventive medicine, medical diagnosis, the provision of health care/treatment (Article 9(h)).	We will use your information for preventive or occupational medicine, for the assessment of the working capacity of the employee (Article 9(h)).

5.7.2 In line with Caldicott 2 recommendations, information will only be shared for the purposes of direct care with registered and regulated health care professionals who have a legitimate relationship with the patient.

5.8 Security of Processing

5.8.1 The Data Protection Act 2018, places an even greater emphasis on organisations to ensure that they have and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, some of which are detailed below and in the Trust's Information Security Policy.

5.8.1 Data Protection Impact Assessments

5.8.1.1 The Trust will ensure that for all new proposed changes to the processing of personal data or special category data, a privacy impact assessment will be undertaken and the company's Data Protection Officer (DPO) consulted to ensure that data protection principles such as data minimisation are integrated into the new processing to protect the privacy rights of data subjects.

5.8.2 Data Processors

5.8.2.1 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. This agreement will outline the data protection responsibilities of both The Trust and the company/supplier.

5.8.3 Encryption

5.8.3.1 In line with the Data Protection Act 2018, The Trust will ensure that all personal data and special category are encrypted when stored on any mobile device, unless these is an overriding clinical need not to encrypt the device e.g. impact on patient care. Where this is the case, these decisions will be agreed and documented at the IG Committee.

5.8.4 Business Continuity /Disaster Recovery Plans

5.8.4.1 The Trust will ensure that it has both business continuity plans and disaster recovery plans in place for all its key/critical assets containing personal data. The Trust will ensure that these plans are tested annually in order to maintain the integrity and availability of the information held.

5.9 Individuals Right

5.9.1 Under the GDPR and Data Protection Act 2018, the rights of individuals have been strengthened and are detailed below:

5.9.1 Right to be informed/transparency

5.9.1.1 All individuals have the right to be informed at the point that the Trust collects information from them and within one calendar month of the Trust receiving the information from a third party company on how the Trust uses their information. To meet this obligation the Trust has developed a patient information leaflet which is displayed in all public facing areas. All outpatient, inpatient and discharge letters sent to patients have the following statement:

5.9.1.2 All information that the Trust holds about you is managed in accordance with the Data Protection Act. For details on how we use your information please visit https://www.fhft.nhs.uk/your-visit/privacy-policy-how-we-use-your-information/

5.9.1.3 The Trust has developed a staff leaflet which is handed to staff at the point that they start working at the Trust.

5.9.2 Right to a copy

5.9.2.1 Under the Data Protection Act 2018, all individuals have the right to obtain a copy of the information held about them by an organisation.

5.9.2.2 Patients are able to exercise their rights by following the Trust's Data Protection Act procedures, which state:

- Patient requests for access to personal data including records must be in writing and addressed to fhft.request.records@nhs.net
- Upon receipt of a request for information together, with two proofs of identification, the Trust will provide to the requester:
  - A copy of all information held by the Trust relating to them, or as requested in their written request e.g. a copy of their x-rays;
  - Details of how the Trust processes their information;
  - The categories of personal data held by the Trust;
  - The recipients with whom their personal data will be shared, including whether any information is shared overseas;
  - The retention period for how long their information is held;
  - The individual's right to rectify, erase, restrict processing of their data;
  - The right to lodge a complaint to the supervisory authority;
  - Where the personal data was provided by a third party, who the source of the data was;
  - Whether any automated decision making, including profiling has been undertaken on their data.

5.9.2.3 If a data subject is unhappy with how the Trust has processed their request for information, they can complain in writing to the Access to Health Records Team Manager in the first instance.

5.9.2.4 Where a patient is dissatisfied with the response to their complaint, they can raise their complaint to the Head of Information Governance / Data Protection Officer. At

this point, if the requester remains unhappy they will be informed of their right as detailed in section 5.9.14 – The right to lodge a complaint with the ICO.

5.9.2.5 The Information Governance Dashboard monitors all patient subject access requests to ensure that they are compiled within the defined timescales in the Data Protection Act 2018.

5.9.2.6 Where staff wish to make a request for a copy of the information held about them by the Trust, this must be sent to the HR Department to be processed. The HR Department will ensure that upon receipt of two proofs of identification, they will provide to the requester:

- A copy of all information held by the Trust relating to them, or as requested in their written request e.g. a copy of their staff file (not payroll)
- Details of how the Trust processes their information.
- The categories of personal data held by the Trust
- The recipients with whom their personal data will be shared, including whether any information is shared overseas
- The retention period for how long their information is held
- The individual's right to rectify, erase, restrict processing of their data
- The right to lodge a complaint to the supervisory authority
- Where the personal data was provided by a third party, who the source of the data was
- Whether any automated decision making, including profiling has been undertaken on their data

5.9.3 Providing a copy

5.9.3.1 In line with Article 15 (3) where the data subject makes a request by electronic means; unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

5.9.3.2. The Trust has moved to electronic documents, so this is the commonly used format within the Trust and will be the format in which all requested information will be provided to a data subject.

5.9.4 Charges for a copy

5.9.4.1 In line with Article 15 (3) the Trust is entitled to charge a reasonable fee based on administrative costs for providing further copies (first copy of information is provided free of charge). Additionally, if a request is too vague, the Trust will ask the data subject to narrow down their request, or if a data subject is requesting a very large amount of information, the Trust may charge for providing a copy as detailed below:

Information	Cost
To send a copy of a CD/X-ray	£10.00
Provide copies of pages 0-100 pages	£10.00
Provide copies of pages 101-200	£20.00

Provide copies of pages 201-300	£30.00
Provide copies of pages 301-400	£40.00
Provide copies of pages 401-500	£50.00

5.9.4.2 Pregnant women who attend the Trust's Ante-natal clinic are offered a service of being able to obtain copies of their baby scan for a charge, which is considered outside of the Data Protection Act 2018, as it is not a copy of the ante-natal report, but a memento of the scan and pregnancy. Therefore, the Trust will continue to charge for this service.

5.9.5 Right to rectification

5.9.5.1 A data subject has the right to request that their personal data is rectified without delay, and have incomplete personal data fully completed. For individuals to exercise this right, they must submit their request to the Data Quality Teams at either Frimley or Wexham Hospital Site.

5.9.5.2 Where the Trust has shared inaccurate data with a third party, they have a legal obligation to inform the third party of the inaccurate data shared and provide them with an accurate copy of the data subject's information.

5.9.5.2 Upon receipt of the request, the Trust will process the request within one calendar month, unless the request is excessive and the Trust requires more time, in which the data subject will be informed that the Trust requires a further month to process their request.

5.9.6 Right to erasure (right to be forgotten)

5.9.6.1 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 from which they were collected
- The data subject objects to the processing, and there is no overriding legitimate grounds for the processing
- The personal data has been unlawfully processed

5.9.6.2 Where the Trust receives a request of this nature it will be passed to the Information Governance Department for consideration, who will provide a response to the data subject on how the Trust has processed their request.

5.9.7 Right to restriction of processing

5.9.7.1 The data subject has the right to request that the Trust restricts processing their data when one of the following applies:

- Accuracy of their personal data is contested
- Processing is unlawful
- The Trust no longer needs the personal data for the purposes of processing
- 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

5.9.7.2 For individuals to exercise this right, they must submit their request to the Information Governance Department. Upon receipt of the request, the Trust will process the request within one calendar month, unless the request is excessive and the Trust requires more time; in which the data subject will be informed that the Trust requires a further month to process their request.

5.9.10 Right to data portability

5.9.11 The data subject has this right, but as the Trust's legal basis for processing an individual's personal data is not reliant on the explicit consent of the data subject, this right is not applicable to the Trust's processing of personal data.

5.9.11 Right to object

5.9.11.1 The data subject has this 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. Upon receipt of the request, the Trust will process the request within one calendar month, unless the request is excessive and the Trust requires more time; in which the data subject will be informed that the Trust requires a further month to process their request.

5.9.12 NHS Opt out

5.9.12.1 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. Details of the national op out in the NHS can be found at: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

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

5.9.13 Right to Automated Decision making / Profiling

5.9.13.1 The data subject has the right not to be subjected to a decision based solely on automated processing, including profiling. As the Trust does not undertake any automated decision making or profiling, this right is not applicable.

5.9.14 Right to lodge a complaint

5.9.14.1 The Trust recognises an individual's right to lodge a complaint with the ICO. This information has been placed on the Trust's website as well as being communicated to patients when they choose to exercise their rights under the Data Protection Act 2018.

5.9.15 Right to compensation

5.9.15.1 The Trust recognises the rights of individuals to seek compensation where they have suffered damage/distress as a breach of the Data Protection Act 2018.

5.10 Accuracy of Data

All staff are responsible for:

- Checking that any patient, staff or other individual's information they access is accurate and up to date.
- Correcting any inaccurate data. This may only be undertaken if the member of staff has sufficient rights to amend data. Otherwise staff must bring the discrepancy to the attention of the system administrator or line manager.
- Checking that any personal information they provide to the Trust in connection with their employment is accurate and up to date, e.g., change of address. The Trust cannot be held responsible for any errors unless the member of staff has informed the Trust.

5.11 Consequences of a breach of the Policy

5.11.1 Breaches of this Policy will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:

- Offences as detailed in the Data Protection Act 2018 (see section 5.12)
- Unlawful disclosure of Personal Data and/or Sensitive Personal Data
- Inappropriate use of Personal Data and/or Sensitive Personal Data.
- Misuse of Personal Data and/or Sensitive Personal Data which results in any claim being made against the Trust.
- Loss of Personal Data and/or Sensitive Personal Data.
- Unauthorised disclosure or copying of information belonging to the Trust

5.12 Offences under the Act

5.12.1 The Data Protection Act 2018 further adds to the offences in the Data Protection Act 1998, which are:

5.12.1 Unlawful obtaining of personal data

5.12.1.1 It is an offence for an individual to knowingly or recklessly

- obtain or disclose personal data without the consent of the data controller
- procure the disclosure of persona data to another individual without the consent of the data controller
- after obtaining personal data, to retain it without the consent of the individual who was the controller in relation to the personal data when it was obtained

5.12.2 Re-identification of de-identified personal data

5.12.2.1 It is an offence for an individual knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the data controller responsible for de-identifying the personal data.

5.12.3 Alteration of personal data to prevent disclosure to a data subject

5.12.3.1 It is an offence for an individual to alter, deface, block erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the persona making the request would have been entitled to receive.

5.13 Reporting Loss of Personal Data

5.13.1 Any breaches/losses of personal data must be reported using the Trust's Incident reporting process and will be reported in the Trust's SIRO report. In line with Article 33 of the GDPR, the company must report any breaches of personal data within 72 hours to the ICO with the following information:

- Nature of the personal breach;
- Categories and approximate number of data subject concerned;
- Name and contact details of the DPO;
- Likely consequences of the personal breach;
- Measures taken or proposed to be taken to address the personal breach.

5.13.2 Additionally, where the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will communicate the personal data breach to the individual without undue delay with the following information and an apology:

- Name and contact details of the Data Protection Officer;
- Likely consequences of the personal breach;
- Measures taken or proposed to be taken to address the personal breach.

5.13.3 NHS Digital is updating the guidance on how the NHS organisations report their data losses. The Trust will continue to follow the NHS digital guidance for reporting its personal data incidents.

5.14 Contracts of Employment

5.14.1 Staff contracts of employment are produced and monitored by the Trust's Human Resources Department. All contracts of employment include an information governance/data protection and confidentiality clause. Agency and contract staff are subject to the same rules.

5.14.2 The Trust has a Confidentiality Agreement that non-Trust staff must sign before undertaking any work in or on behalf of the Trust.

6. DUTIES / ORGANISATIONAL STRUCTURE

6.1 The Chief Executive Officer

The Chief Executive Officer has overall responsibility for the Data Protection Policy within the Trust. The implementation of, and compliance with, this Policy is delegated to the Head of Information Governance as the Trust's designated Data Protection Officer.

6.2 Caldicott Guardian

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 Trust's Caldicott Guardian is the Medical Director.

6.3 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 and provide written advice to the Accounting Officer on the content of their Statement of Internal Control in relation to information risk. The Trust's SIRO is the Director of Finance & Strategy.

6.4 The Head of Information Governance

The Head of Information Governance is the Trust's designated Data Protection Officer.

6.4.1 The Trust Data Protection Officer's role includes:

- 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
- Ensuring staff undertake annual IG training
- Provide advice for staff when completing a Data Protect 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

6.5 General and Clinical Managers / Heads of Department / Information Asset Owners (IAO)

6.5.1 Data Protection procedures will vary from Department to Department and across disciplines. It is the responsibility of General Managers / Clinical Managers / Heads of Department to ensure that adequate and compliant procedures are developed to handle personal data and sensitive personal data.

6.5.2 General / Clinical Managers and Heads of Department may delegate the day to day running of operational procedures but may not delegate overall responsibility for the handling of personal data and sensitive personal data within their Departments.

6.5.3 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.

6.5.4 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.

6.6 Information Asset Administrators (IAA)

6.6.1 Each computer system/database will have a designated application and/or System Manager/Information Asset Administrator. A list of these nominated personnel will be maintained as part of the Asset inventory which forms part of the Trust's Information Security Management System.

6.6.2 All Information Asset Administrators will ensure that all systems/databases which require registration are registered in accordance with the Data Protection Act's requirements and these registrations are reviewed on a regular basis.

6.6.3 The day to day responsibility for enforcing the Policy will be devolved to the application managers and other nominated personnel. In order to fulfil their roles, the Head of Information Governance will ensure that regular training is provided to remind these personnel of their responsibilities and advise the most effective way of ensuring adequate information security and confidentiality.

6.7 Members of staff responsibilities

6.7.1 All employees of the Trust who process personal data in any form must ensure that they comply with:

- The requirements of the Data Protection Act 2018;
- The Trust's Data Protection and Confidentiality Policy, including any procedures and guidelines which may be issued from time to time.

6.7.2 All staff are responsible for ensuring that they attend Information Governance Training to understand the key principles of the Data Protection Act and how this applies to Trust policies, procedures and guidance.

6.7.3 All queries about the Trust Policy should be directed to the Head of Information Governance.

7 RAISING AWARENESS / IMPLEMENTATION / TRAINING

As part of the induction process, both corporate and departmental, all Trust employees will be made aware of their responsibilities in connection with the Acts mentioned in this Policy. This will be provided through their Statement of Terms and Conditions and targeted training sessions carried out by Application Managers and/or other trainers/specialists.

8 MONITORING COMPLIANCE OF POLICY

The Trust will monitor staff compliance against this policy through the monitoring of reported Trust incidents, audits of staff working practices relating to breaches of confidentiality, loss of personal information.

9 EQUALITY IMPACT ASSESSMENT

This Policy has been subject to an Equality Impact Assessment and is not anticipated to have an adverse impact on any group.

10 REFERENCES

- Data Protection Act (2018)
- General Data Protection Regulations (GDPR)
- The Department of Health Confidentiality Code of Practice (2003)
- Information Commissioners Office
- Department of Health Report on the Review of Patient-Identifiable Information (1997)
- Connecting for Health Off-Shore Policy

Appendix A

Data Protection Act 2018 Principles

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

Principle 1 – "Personal data shall be processed fairly, lawfully and in a transparent manner"

Fair Processing

There is a requirement to make the general public, who may use the services of the Trust, aware of why the Trust needs information about them, how this is used and to whom it may be disclosed.

This requires the Trust to make sure individual understand how their information is to be used to support their healthcare and that they have no objections.

Where staff are not able to answer a patient's queries on how their information is used, they should be referred to either the Trust's Patient Advisory Liaison Service (PALS) or the Trust's Information Governance Department.

Transparent

The Trust needs to make it transparent to patients who their information is being used. All leaflets which are provided to patients by the Trust will be clear and transparent on how their information is being used and shared to support their care. These leaflets will be easily accessible, easy to understand using clear and plan language.

Patients

Patients will be made aware of this requirement by the use of Trust Data Protection Leaflet, statements in other Trust leaflets/handbooks/survey forms and verbally by those health care professionals providing care and treatment.

The Trust will keep up to date a page on the Frimley Health Internet site. This will provide more detailed information on how the Trust uses patient information.
https://www.fhft.nhs.uk/your-visit/privacy-policy-how-we-use-your-information/

Staff

The Trust will issue all staff with a leaflet that details how the Trust uses their information.

Principle 2 - "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes"

All databases which hold and/or process personal information about living individuals must be registered with the Trust's Information Governance department, which will inform the Trust's Record of Processing activities.

For the purposes of Data Protection, a database is considered to be any collection of personal information (more than 51 records) that can be processed by automated means, e.g.,

- Patient records (names and addresses etc.) for appointments
- Patient details used for prescribing drugs
- Patient information used for research, e.g., where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this could be a spreadsheet or Access database
- Staff records held on Excel to monitor annual leave and sickness

When collecting personal information, it is essential that the data subject is clear about why the information is being collected and what the information is to be used for. The same information can be used for several different purposes as long as the data subject has been made aware of all of these purposes.

Principle 3 – "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Information collected from individuals should be complete and should all be justified as being required for the purpose for which they are being requested. Information must not be collected because it might be useful at a future date.

Principle 4 – "Personal data shall be accurate and, where necessary, kept up to date"
The Trust has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific, and details must be provided of these validation processes to the system/information users.

Users of software will be responsible for the quality (i.e., Accuracy, Timeliness, Completeness) of the data held in their software/systems and must carry out quality assurance audits.

All staff must check with patients that the information held by the Trust is kept up to date; this can be achieved by asking patients attending appointments or coming into the hospital to validate the information held by the Trust.

Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/Personnel department.

There may be instances when non-current information needs to be retained, e.g., for audit purposes or historical research, where this is the case, the information must be correct at the time it was recorded.

Principle 5 – "Personal data kept for no longer than is necessary for the purposes for which the personal data are processed"
All records containing personal information must only be stored for the appropriate length of time. The "DH Records Management: NHS Code of Practice" provides comprehensive guidance for NHS organisations on the retention period for all NHS records. Further details of how this affects the Trust, and actions required to comply with it, are detailed in the Trust's Records Management Policies.

If the information on the computer or manual record is not the main record, this is considered to be transient data. The Trust will develop procedures/ guidance for staff to know and understand what information should be culled, archived or destroyed when no longer deemed to be of use.

The Trust has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and Trust business. It is important that this information is disposed of in a secure manner.

Principle 6 – "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

All information relating to identifiable individuals must be kept secure at all times. The Trust will implement policies/procedures to protect Trust information against unauthorised processing of information, accidental loss, destruction and damage to this information. Measures being undertaken are:

- All removal media will be encrypted
- All laptops will be encrypted.
- All software and data is removed from redundant hardware and media storage (e.g., tapes, disks) before the hardware is removed from the Trust.
- Confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.
- Staff will not share user names and passwords.
- Trust will implement systems that have appropriate security measures and functionality.

Information Asset Administrator

Each Information Asset Administrator is responsible for ensuring that the system they manage complies with the Data Protection Act. This responsibility includes keeping the system security policy up to date and ensuring procedures are in place to achieve a high level of data security and quality.

Each Information Asset Administrator is responsible for ensuring:

- the Data Protection registrations/notifications are up to date
- users are set up on the system on a need to know basis
- unusual requests for disclosure are scrutinised
- staff are aware of their responsibilities regarding security, data protection and confidentiality issues

Back-ups

Each Information Asset Administrator is responsible for ensuring the system they are responsible for is regularly backed up.

Some of the Trust IT Systems will have their systems backed up on a daily basis by the IT Department. The master copy of programs and back-ups of data will be kept securely by the IM&T departments.

Disclosure of information/information in transit
Information about identifiable individuals (such as patients and staff) must only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

However, some disclosures of information may occur because there is a statutory requirement upon the Trust to disclose, e.g., Court Order; other legislation requires disclosure, e.g., tax office, pension agency - for staff; notifiable diseases - for patients.

Only Trust approved transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturer's specifications.

Contracts
Contracts between the Trust and third parties should include the Trust's standard confidentiality clause, which should be disseminated to the third party's employees.

Caldicott Principles

Principle 1: Justify the purpose(s).
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by the appropriate guardian.

Principle 2: Don't use personal confidential data unless it is absolutely necessary.
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3: Use the minimum necessary personal confidential data.
Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function.

Principle 4: Access to personal confidential data should be 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.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities.
Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibility and obligations to respect patient confidentiality.

Principle 6: Comply with the law.
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidentiality data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality.
Health and Social care professional should have the confidence to share information in the best interest 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.