

## TRUST POLICY AND PROCEDURE FOR DATA PROTECTION AND DEALING WITH CONFIDENTIAL INFORMATION

<b>Reference Number</b> POL-IG/1294/08	<b>Version:</b> V3		<b>Status</b> Final	<b>Author: Anne Woodhouse</b>  <b>Job Title:</b> Head of Information Governance
Version / Amendment History	Version	Date	Author	Reason
	V3	May 2018	Anne Woodhouse	Review and amendments
	V4	May 2021	Anne Woodhouse	Review and minor amendments
<b>Intended Recipients:</b> All staff, students or volunteers working in the Trust. This includes all third parties and contractors				
<b>Training and Dissemination:</b> Via the intranet, IG mandatory training, Induction, Directorate Mandatory Training Days and e-learning				
<b>To be read in conjunction with:</b> <ul style="list-style-type: none"> <li>• Information Governance - Trust Policy and Procedure</li> <li>• Disciplinary of Employees</li> <li>• Information Technology and Cyber Security</li> <li>• Mobile Devices / Mobile and Landline Telephony</li> <li>• Data Protection and Confidentiality (Dealing with Confidential Information) -</li> <li>• Waste Management Policy</li> <li>• Access to Personal Data Policy</li> </ul>				
<b>In consultation with and Date:</b> Information Governance Steering Group May 2021				
<b>EIRA stage One Completed</b>		Yes		
Stage Two Completed		No		
<b>Approving Body and Date Approved</b>			Information Governance Steering Group May 2021	
<b>Date of Issue</b>			May 2021	

<b>Review Date and Frequency</b>	May 2022 (then every three years)
<b>Contact for Review</b>	Head of Information Governance
<b>Executive Lead Signature</b>	Executive Medical Director
<b>Approving Executive Signature</b>	Executive Medical Director

## CONTENTS

<b>Section</b>		<b>Page</b>
1	Introduction	4
2	Purpose	4
3	Definitions Used	4
4	Key Responsibilities / Duties	5
5	Implementation of the Policy	6
6	Monitoring Compliance and Effectiveness	11
7	References	12

## 1. Introduction

University Hospitals of Derby and Burton NHS Foundation Trust (the Trust) has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner and professional bodies. Penalties could be imposed on the Trust or its employees for non-compliance.

Any staff member working or volunteering in the Trust will come into contact with confidential information / data relating to the work of the Trust, its patients or staff. All staff have a legal duty to keep this information confidential. This applies to information manually created and held, created and stored on computer systems, and also any verbal information received or overheard.

## 2. Purpose

The purpose of this Policy is:

- To ensure staff, contractors and volunteers comply with all relevant legislation and guidance:
  - The General Data Protection Regulation (GDPR)
  - Data Protection Act (DPA) 2018
  - The Caldicott Principles
  - The Human Rights Act 1998
  - The NHS Confidentiality Code of Practice DH 2003
  - Data Security & Protection Toolkit (DSPT)
  - Freedom of Information Act 2000
- To protect staff, contractors and volunteers by making them aware of correct procedures when dealing with confidential information
- To ensure staff, contractors and volunteers understand their responsibilities when dealing with confidential information
- To ensure patient information is used only for the purpose for which it was given and not divulged without the patients consent unless for a lawful purpose.

This Policy has been produced to ensure the Trust is able to fulfil its duties as a health care provider whilst maintaining the rights of individuals in respect of their personal details.

## 3. Definitions Used

<b>Data</b>	Data under the Act means information which: <ul style="list-style-type: none"><li>• Is being processed electronically e.g. information systems, databases, including microfiche, audio and video systems (CCTV) and telephone logging systems</li><li>• Is recorded with the intention that it shall be processed by equipment</li><li>• Is recorded as part of a relevant filing system e.g. manual files and records forming part of a relevant filing system structured</li></ul>
-------------	--

either by reference to individuals or criteria relating to individuals

- Is an accessible record summarised as a health record.

<b>PID</b>	Person Identifiable Data
<b>Personal Data</b>	Personal data as defined by the law: <i>'Data which relates to a living individual who can be identified.'</i> Personal data now includes a range of personal identifiers – name, identification number, location data, and online identifiers. Pseudonymised data can fall within the scope depending on how difficult it is to attribute the pseudonym to a particular individual.
<b>The Legislation</b>	The General Data Protection Regulation (GDPR) and UK Data Protection Legislation.
<b>Processing</b>	Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: <ul style="list-style-type: none"><li>• Organisation, adaptation or alteration</li><li>• Retrieval</li><li>• Disclosure</li><li>• Erasure or destruction</li><li>• Viewing personal information or data, even where no changes are made.</li></ul>
<b>Special category data</b>	Information related to a data subject's: <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious beliefs or beliefs of a similar nature</li><li>• Trade union membership</li><li>• Physical or mental health or condition</li><li>• Sexual life</li><li>• Offences or alleged offences and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.</li></ul>
<b>Data Controller</b>	The individual, company or organisation that determines the purpose and the manner in which personal data may be processed. The Data Controller is the Trust.
<b>Data Processor</b>	Data Processor in relation to personal data, means any other person other than an employee of the Trust who processes data on behalf of the Trust

#### 4. Key Responsibilities / Duties

**4.1 The Caldicott Guardian** is a senior person responsible for protecting the confidentiality of a patient and service-user information. This includes representing and championing

confidentiality requirements at Board level. The Caldicott Guardian is the Executive Medical Director.

**4.2 The Senior Information Risk Owner (SIRO)** is responsible for the ownership of information risk across the Trust. The SIRO acts as advocate for information risk to the Trust Board and is the Director of Finance and Performance.

**4.3 The Director of IM&T** is responsible for the overall implementation of relevant changes to Policy and Procedure.

**4.4 The Head of Information Governance** is responsible for acting as the initial point of contact for any data protection / confidentiality issues that may arise within the Trust. This includes the transfer of PID. They will also be responsible for notifying the Information Commissioner of the purposes for which the Trust processes personal data and reporting Serious Incidents to the Information Commissioner and the Department of Health.

**4.5 The Data Protection Officer (DPO)**. GDPR introduces a duty for all public authority organisations to appoint a DPO. The DPO is responsible for informing and advising the organisation about its obligations to comply with the GDPR and other data protection laws. The DPO will be responsible for monitoring compliance with relevant laws, and internal data protection policies, including managing internal data protection activities. The DPO will cooperate with the supervisory authority and be the first point of contact for supervisory authorities and for individuals whose data is processed.

**4.6 The Information Governance Steering Group (IGSG)** is responsible for monitoring this Policy and receiving regular reports regarding breaches of confidentiality. The IGSG will also monitor compliance with and work towards resolving issues connected with the DPA.

#### **4.7 Managers**

All managers must ensure that staff are aware of and comply with this Policy and all relevant guidance. They are also responsible for ensuring staff compliance with annual IG training.

**4.8 All staff, third parties and contractors** are expected to adhere to this Policy and ensure that all patient / personal information is accurate, up to date and that it is kept secure at all times. They must also attend Information Governance training annually.

### **5. Implementation of the Policy**

#### **5.1 Data Protection Legislation**

The Trust has an obligation as Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. The Data Protection Legislation requires that personal data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes shall not be considered to be incompatible with the initial purposes

- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the 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 GDPR in order to safeguard the rights and freedoms of individuals; and
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The legislation requires a Data Protection Impact Assessment to be carried out for all projects or changes to procedures that involve the processing of personal data.

#### Processing of personal data

The legislation requires you to determine your lawful basis before you begin processing and this must be documented. There are six available lawful bases for processing. These are:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- The processing is necessary for the performance of a contract to which the data subject is party
- The processing is necessary for compliance with a legal obligation to which the controller is subject
- The processing is necessary in order to protect the vital interests of the data subject or of another natural person
- The processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child – this basis cannot be used by public authorities

Processing of special category data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic and biometric data, health data or data concerning a person's sexual orientation) shall be prohibited unless one of the following apply:

- (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 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;
- (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.

## **5.2 The Caldicott Principles**

The original Caldicott Report, published in 1997, established six principles for NHS bodies (and parties contracting with such bodies) to adhere to in order to protect patient information and confidentiality. Over recent years there has been 2 further Caldicott Principles added bringing the total of Caldicott Principles to 8.

The Trust must comply with the Caldicott Principles, which state:

- Use of personally identifiable information must always be justified
- Personally identifiable information must not be processed unless absolutely necessary
- Where it is not possible to remove all personal identifiable information, the amount used must be kept to a minimum
- Personally identifiable information must only be used on a need to know basis
- All users of personally identifiable information must be aware of their responsibilities
- All users of personally identifiable information must understand and comply with the law
- 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
- Inform patients and service users about how their confidential information is used. A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate.

## **5.3 Disclosure of information**

Under Data Protection legislation, Human Rights Act and NHS Caldicott Guidance, staff are under a duty of confidence to keep personal / sensitive information confidential and secure.

However, there are circumstances where the Trust may be required to disclose information to external agencies / bodies without the consent of the individual. Some examples are, in response to a court order, to assist the police with serious enquiries when it is in the public's best interest and in the case of child protection / safeguarding issues.

Prior to disclosing information advice and guidance **MUST** be sought from the Information Governance team on via switchboard.

More guidance can be found within the IG section on the Trust Intranet - Netl.

## **5.4 Disclosure of Information outside the European Economic Area (EEA)**

Personal information must not, unless certain exemptions apply or protective measures are taken, be disclosed or transferred outside the EEA or to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

In the event that any member of staff wishes to process personal information outside of the United Kingdom, the Information Governance team must be consulted prior to any agreement to transfer or process information.

## **5.5 Transportation of information**

- In certain circumstances it may be necessary to transport PID in hard copy format or on portable media, e.g. USB sticks and laptops. The portable media must be encrypted and staff must comply with the Mobile Devices / Mobile and Landline Telephony. Confidential information, hard copy and electronic, must never be left unattended. For more detail please see the procedures and best practice guidance within the IG section on Net-i or contact the Information Governance team.

## **5.6 Use and Sharing of information**

Staff must not access any information that they do not have a legal right to access, i.e. only access personal information in line with work or if are involved in their care. Individuals will be in breach of Data Protection law and liable to disciplinary or criminal proceedings by accessing information about a relative, friend, neighbour or colleague. Staff do not have the right to access their own information, there are clear processes for access to personal information – please refer to the Access to Personal Data Policy for more information.

Patients must be made aware of why their information is being collected, how it will be used and who this will be shared with.

GDPR gives enhanced rights to individuals about the use of their personal data:

- The right to be informed
- The right to access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Patients have the right to object to the sharing of their information; however they need to be made aware that it is essential that their data is processed in order to provide the best possible care and if they refuse to allow it to be shared with other health professionals this could impact on their care.

The right to access does change the process for dealing with Subject Access Requests. The timescale for dealing with these requests has reduced from 40 days to 1 calendar

month and there can be no charge for processing these requests unless the request is manifestly unfounded or excessive, particularly if it is repetitive.

Confidential information must not be saved to the desktop or hard drive of computers. Trust secure network drives must be used to ensure the security of the data.

Confidential information must be disposed of under confidential conditions – please refer to the Trust Waste Management Policy.

### **5.7 Contracts of employment**

All contracts of employment must include a data protection and general confidentiality clause. Agency and non-contract staff working on behalf of the Trust must be subject to the same rules. All staff will be made aware of their responsibilities through their Statement of Terms and Conditions.

### **5.8 Training**

The successful implementation of this Policy is dependant on trust wide awareness raising and continual monitoring of employees understanding of confidentiality. It is a requirement that all staff, volunteers and contractors undertake annual IG training, with additional training being delivered to specific categories of staff.

### **5.9 Mobile Computers / Photography**

Only Trust equipment or equipment registered to medical photography can be used. It is prohibited to use non-trust equipment or mobile computers (e.g. mobile phone, tablet) to take patient images or to photograph information relating to a patient or their treatment. If it is deemed essential, with no other options available, images can be taken using an encrypted mobile device, however the device must not be synched to cloud services. Images must never be sent over a mobile phone network. The image must be deleted as soon as possible.

There must be a fully justifiable purpose for a visual image to be carried out and consent must be obtained

## **6. Monitoring Compliance and Effectiveness**

Monitoring Requirement :	Compliance with the DSPT – all requirements must be at level 2.  Compliance with mandatory training – Trust target 95% annually Monitoring of Information Governance Incidents – Serious Incidents will be reported to the Information Commissioner and the Department of Health, which is done through the DSPT.  These will be summarised in the statement of internal control in the annual report.
Monitoring Method:	The collection of evidence to support scores for requirements. The DSPT is populated with evidence and is audited annually

	Learning and Development will provide monthly reports regarding compliance within all directorates  Incidents are reported via Datix.
Report Prepared by:	Head of Information Governance
Monitoring Report presented to:	Information Governance Steering Group  Information Governance Action Group  Incident Learning Group
Frequency of Report	Training compliance – Monthly  IG / Incidents - Quarterly

Where deficiencies are highlighted, action plans will be formulated and monitored for improvements.

## 7. References

Source of data	Date of publication / issue	Detail of requirement
The General Data Protection Regulation	2018	
UK Data Protection legislation	2018	
NHS Caldicott Guidance	2018	
Confidentiality: NHS Code of Practice		
The Information Commissioner		
<a href="http://www.ico.gov.uk/">http://www.ico.gov.uk/</a>		
Prevention of Terrorism Act	1989	
Terrorism Act	2000	
Crime and Disorder Act	1984	
The Police and Criminal Evidence Act	1984	