University Hospitals Bristol and Weston
NHS Foundation Trust

Confidentiality Policy

Document Data			
Document Type:	Policy		
Document Reference:	23466		
Document Status:	Approved		
Document Owner:	Information Governance		
Executive Lead:	Director of Finance and Information		
Approval Authority:	Risk Management Group		
Review Cycle:	36 Months		
Date Version Effective From:	8 October 2022	**Date Version Effective To:**	7 October 2025

What is in this policy?

The Confidentiality Policy explains the balance of maintaining the confidentiality of personal information across the Trust with the need the share this information with other organisations that require it.

All personal information concerning patients or employees of the Trust should be treated as confidential.

Document Change Control				
Date of Version	**Version Number**	**Lead for Revisions**	**Type of Revision**	**Description of Revision**
Jan 2018	0.1	Information Governance Officer	Major	Initial draft
Aug 2019	0.2	Information Governance Officer	Minor	Update of references and links to other procedural documents.
Sep 2019	0.3	Information Governance Officer	Minor	Amendments to roles and responsibilities.
Sep 2019	1.4	Information Governance Officer	Minor	Amendments requested by the Policy Assurance Group
Sep 2022	2.0	Information Governance Officer	Minor	Update of references and links to other procedural documents. Amendments to roles and responsibilities.

Sign off Process and Dates	
Groups consulted	**Date agreed**
Information Risk Management Group	30/09/2022
Policy Assurance Group	20/09/2022
Risk Management Group	8 October 2022

- **Stakeholder Group** can include any group that has been consulted over the content or requirement for this policy.
- **Steering Group** can include any meeting of professionals who has been involved in agreeing specific content relating to this policy.
- **Other Groups** include any meetings consulted over this policy.
- **Policy Assurance Group** must agree this document before it is sent to the **Approval Authority** for final sign off before upload to the DMS.

Table of Contents

Do I need to read this Policy?

All staff

Must read the whole policy

Introduction

The Confidentiality Policy explains the balance of maintaining the confidentiality of personal information across the Trust with the need to share this information with other organisations that require it.

1. Purpose

This policy is designed to highlight to staff their responsibilities in respect of the confidentiality of personal information and in respect of sharing personal information appropriately.

This policy is not a definitive or exhaustive guide to confidentiality or information sharing and does not replace or override any of the guidance or codes on conduct written by professional bodies.

2. Scope

This document applies to all staff across the Trust and provides the overarching framework for maintaining and sharing confidential information.

3. Definitions

3.1 Confidentiality

Information is only available to those who need it and can only be disclosed to those who are authorised to receive it, by those authorised to release it.

3.2 Personal Information

Factual information or expressions of opinion, which relate to an individual who can be identified from that information or in conjunction with any other information coming into the possession of the holder of that information.

3.3 Common Law

A part of English Law that is derived from judicial decisions of courts or similar tribunals rather than in written statutes.

3.4 Information Asset

A body of information that is defined and managed as single entity. This includes IT systems, databases and paper records.

4. Duties, Roles and Responsibilities

4.1 Trust Board of Directors

(a) To oversee the Trust's policy in respect of information governance taking legal and NHS requirements into account

(b) To ensure sufficient resources are provided to support the requirements of this policy.

4.2 Director of Finance & Information

(a) To fulfil the role of Senior Information Risk Owner (SIRO)

(b) To take overall strategic ownership of this policy

4.3 Caldicott Guardian

(a) To fulfil the role of Caldicott Guardian

(b) To assess and approve all procedures that relate to the processing of personal information in line with the Caldicott Principles

(c) Current post holder is Consultant Paediatric Accident and Emergency

4.4 Senior Leadership Team

(a) To develop, manage and implement this policy

4.5 Information Asset Owners/Administrators

(a) To map, manage and review information flows for their information asset for compliance with this policy

(b) To ensure that only staff who need to have access to information held on their asset can do so

(c) To keep their asset up to date on the Trust's Information Asset Register

4.6 Head of Risk and Information Governance

(a) To fulfil the role of the Data Protection Officer

(b) To monitor ongoing compliance with General Data Protection Regulation 2016 and the Data Protection Act 2018

(c) To implement, develop and monitor the Information Governance agenda

4.7 All Line Managers

(a) To ensure this policy is built into local processes

(b) To ensure ongoing understanding and compliance from staff members

4.8 All Staff

(a) To only access personal information, they are required to as part of their employment

(b) To not access the records of friends, family members, notable individuals or themselves

(c) To share information according to best practices only

5. Policy Statement and Provisions

This is the main part of the policy, which lays out the specific information regarding following the policy. This is not a space for procedures, which should be set up as separate Standard Operating Procedures (SOPs) and added to the DMS separately (and referenced below).

5.1 Duty of Confidentiality

Under the "Common Law Duty of Confidence," any personal information given or received in confidence for one purpose may not be used for a second purpose or shared with anyone else without the consent of the data subject. There are two exceptions to the duty of confidentiality; information may be disclosed without the consent of the individual if:

- There is an overriding public interest in the disclosure
- There is a legal requirement to disclose the information

The duty of confidentiality continues after a patient has died, access to and sharing of these records remain under the same protections.

As UK GDPR does not apply to deceased individuals, access by 3rd parties to deceased records is governed by the Access to Health Records Act 1990.

5.2 Collecting Personal Information

Personal information must only be collected for a specified purpose and be collected fairly and lawfully.

Only the minimum amount of personal information needed to satisfy the specified purpose must be collected and recorded.

5.3 Handling Personal Information

All personal information should be treated as confidential and only be used for the purposes for which it was given.

All staff will come into contact with personal information in the course of their employment and it is their responsibility to ensure that the confidentiality of this information is maintained.

5.4 Access to Personal Information

Staff must only access information that they need to as part of their employment. Staff must not look up or read information about a patient or staff member unless they are involved in their direct care or administration; this includes a staff member accessing their own records.

Staff must only access personal information held on computer systems through their own accounts and usernames. Passwords and usernames must not be shared with colleagues and no attempt to access information on a colleague's account should be made. All access to information is auditable and staff will be held responsible for access on their account, whether they accessed it or not.

Computer screens and printer trays should be situated out of sight of the general public and no personal information must be left on show when these are unattended. Staff must always log off or lock the PC before leaving it unattended and utilise the Secure Print queues around the Trust.

5.5 Storage of Personal Information

Records containing personal information must never be left unattended where they are accessible to patients, visitors and other members of public. Records that are not being worked with must be stored in locked cabinets and drawers, and the keys to these must be kept secure. Offices must be locked when they are unoccupied.

Confidential information must never be stored on:

- Unencrypted removable media devices – e.g., USB sticks, mobile phones
- Personal email accounts – e.g., Hotmail, doctors.net, Gmail
- Cloud Storage Sites – e.g., Dropbox, iCloud
- Google Drive, sheets, documents

Confidential information should only be taken off-site when it is absolutely necessary, e.g., staff working in community clinics, and must be properly secured at all times. All other staff must check that they are not taking confidential information off-site before leaving the Trust, and either dispose of it in confidential waste bins or return it to the relevant department.

Staff members are responsible for any portable IT equipment assigned to them and must ensure that is kept away from any source of potential damage, loss or theft.

5.6 *Disposal of Personal Information*

Records containing personal information must be disposed of according to the Records Management & Retention Policy and the Waste Disposal Policy.

Any IT equipment, including CDs, DVDs, VHS Tapes and floppy disks must be directed to the IM&T ServiceDesk.

5.7 *Information Sharing*

The seventh Caldicott Principle, introduced in 2013, says:

“The duty to share personal information can be as important as the duty to protect patient confidentiality”

This creates a duty for health and social care professionals to share information in the best interests of their patients within the framework of the first six Caldicott Principles.

The sharing of information can take many forms:

- A reciprocal exchange of information
- One or more organisations providing information to a third party or parties
- Several organisations pooling information and making it available to each other
- Several organisations pooling information and making it available to a third party or parties
- Exceptional one-off disclosures of information in unexpected or emergency situations

5.8 *Transfer of Personal Information*

In all circumstances of information sharing, the transfer of the information must always comply with laws, guidance and best practice.

Any transfer of information must be conducted securely with an adequate level of protection. It is the responsibility of each staff member to ensure that personal information is transferred securely.

The Trust’s Secure Transfer of Information SOP details how information can be sent securely, but general provisions are listed below:

Post

The Royal Mail is deemed secure for the transfer of person identifiable information.

Email/Removable Media

Data transferred electronically, either by email or using portable storage media must be encrypted to [redacted].

Secure email pathways are listed in the Secure Transfer on Information SOP and on the Information Governance Connect site.

Telephone

Care must be taken when using telephones. All staff should confirm, as far as reasonable possible, that the person they are speaking to is who they say they are and that they have a legitimate need for the information they are requesting. Staff should not leave confidential information in answerphone messages.

Fax

Fax machines are an insecure method of transmission and should only be used to transfer personal information in an emergency scenario where delay would cause harm to the patient.

Fax messages should contain only the minimum personal information necessary.

5.9 Disclosure of Personal Information

Personal information must only be shared on a need-to-know basis. Care must be taken to ensure that the disclosure of the information is for an authorised purpose. Any doubts should be raised with your line manager and the Information Governance team.

Staff should not discuss personal information when the conversation can be overheard if it can be avoided and must not discuss personal information with those who do not have a legitimate need for that information.

Individuals have the right to request copies of information about themselves by making a Subject Access Request. Patients can request copies from Home Page - [redacted] and staff members can contact Employee Services for copies of their personnel file.

5.10 Managing Confidentiality Breaches

Any breach of confidentiality is an information governance incident and must be reported on the Trust’s incident reporting system, Datix as soon as staff members become aware of the breach.

Incidents will be managed in line with the Trust’s Policy for the Management of Incidents.

Staff members that deliberately, maliciously or breach confidentiality may be subject to disciplinary action in line with the Trust’s Disciplinary Policy.

6. Standards and Key Performance Indicators

6.1 Applicable Standards

The organisation undertakes to comply with the following legal acts and the NHS regulations:

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Crime & Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
- Freedom of Information Act 2000 (& Re-use of public sector information regulations)

In addition to the above, other legislation can impact upon the way in which we should use information. This includes:

- Children Act (1989 & 2004)
- Public Interest Disclosure Act 1998
- Audit & Internal Control Act 1987
- NHS Sexually Transmitted Disease Regulations 2000
- National Health Service Act 1977
- Human Fertilisation & Embryology Act 1990
- Abortion Regulations 1991
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health & Safety at Work Act 1974

6.2 Measurement and Key Performance Indicators

Compliance with the policy will be monitored by the number of reported Information Governance Incidents on Datix, and proactive audits of access to records on Trust IT systems in line with the Audit & Acceptable Use SOP.

7. References

There are no external references.

8. Associated Internal Documentation

[redacted]

9. Appendix A – Monitoring Table for this Policy

The following table sets out the monitoring provisions associated with this policy. Please ensure any possible means of monitoring this policy to ensure all parts are fulfilled are included in this table. **The first line is an example for you and should be removed prior to submission.**

Objective	Evidence	Method	Frequency	Responsible	Committee
Monitoring of incidents to identify learning.	Incident reports from Datix Incident Reporting System.	Data extraction from incident reporting system.	Quarterly, Annually and Ad hoc as required.	Divisional Health and Safety Leads/Divisional H&S (site/service) Advisors	Trust Health and Safety Committee/Divisional H&S Forums.
Discover inappropriate access to records.	Records Access Audits from Trust IT systems.	Data extraction from Trust IT systems.	Monthly	System Managers	Information Risk Management Group

10. Appendix B – Dissemination, Implementation and Training Plan

The following table sets out the dissemination, implementation and training provisions associated with this Policy.

Plan Elements	Plan Details
The Dissemination Lead is:	Information Governance Manager
Is this document: A – replacing the same titled, expired policy, B – replacing an alternative policy, C – a new policy:	C
If answer above is B: Alternative documentation this policy will replace (if applicable):	[DITP - Existing documents to be replaced by]
This document is to be disseminated to:	Newsbeat
Method of dissemination:	Newsbeat
Is Training required:	Yes
The Training Lead is:	Information Governance

Additional Comments
[DITP - Additional Comments]

11. Appendix C – Equality Impact Assessment (EIA) Screening Tool

Further information and guidance about Equality Impact Assessments is available here:

[redacted]

Query	Response
What is the main purpose of the document?	This policy is designed to highlight to staff their responsibilities in respect of the confidentiality of personal information and in respect of sharing personal information appropriately.
Who is the target audience of the document? Who is it likely to impact on? (Please tick all that apply.)	Add ☑ or ☒ **Staff**

Could the document have a significant negative impact on equality in relation to each of these characteristics?	YES	NO	Please explain why, and what evidence supports this assessment in relation to your response.
Age (including younger and older people)		X	Confidentiality is protected for all individuals.

Disability (including physical and sensory impairments, learning disabilities, mental health)		X	Confidentiality is protected for all individuals.
Gender reassignment		X	Confidentiality is protected for all individuals.
Pregnancy and maternity		X	Confidentiality is protected for all individuals.
Race (includes ethnicity as well as gypsy travelers)		X	Confidentiality is protected for all individuals.
Religion and belief (includes non-belief)		X	Confidentiality is protected for all individuals.
Sex (male and female)		X	Confidentiality is protected for all individuals.
Sexual Orientation (lesbian, gay, bisexual, other)		X	Confidentiality is protected for all individuals.
Groups at risk of stigma or social exclusion (e.g., offenders, homeless people)		X	Confidentiality is protected for all individuals.
Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)		X	Confidentiality is protected for all individuals.

Could the document have a significant positive impact on inclusion by reducing inequalities?	**YES**	**NO**	**If yes, please explain why, and what evidence supports this assessment.**
Will it promote equal opportunities for people from all groups?		X	No effect.
Will it help to get rid of discrimination?	X		Effective protection of confidentiality for protected groups reduces the risk of discrimination from information being made publicly available.
Will it help to get rid of harassment?	X		Effective protection of confidentiality for protected groups reduces the risk of harassment from information being made publicly available accidentally or maliciously.
Will it promote good relations between people from all groups?		X	
Will it promote and protect human rights?	X		Right to privacy under the Human Rights Act.

On the basis of the information/evidence so far, do you believe that the document will have a positive or negative impact on equality? (Please rate by circling the level of impact, below.)

Positive impact				**Negative Impact**		
Significant	[✓ **Some**]	Very Little	NONE	Very Little	Some	Significant

Will the document create any problems or barriers to any community or group? NO

Will any group be excluded because of this document? NO

Will the document result in discrimination against any group? NO

If the answer to any of these questions is YES, you must complete a full Equality Impact Assessment.

Is a full equality impact assessment required? NO

Date assessment completed:

Person completing the assessment:

12. Appendix D – Evidence of Learning from Incidents

The following table sets out any incidents/ cases which informed either the creation of this document or from which changes to the existing version have been made.

Incidents	Summary of Learning