Torbay and South Devon
NHS Foundation Trust

Code of conduct for employees in relation to confidentiality

Document Information

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

Date of Issue:	February 2026	Next Review Date:	September 2026
Version:	5	Last Review Date:	February 2025
Author:	Information Governance Officer		
Director Responsible	Director of Corporate Governance & Trust Secretary		
Approval Route			
Approved By:		Date Approved:	
Information Governance Operational Group		February 2026	
Information Governance Steering Group		February 2025	
Information Governance Steering Group		February 2024	
Information Governance Steering Group		February 2023	
Links or overlaps with other policies:			
• Information Governance Policy • Individual Information Rights Policy • Disciplinary Policy (H1)			
We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership. We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy.			

Amendment History

Issue	Status	Date	Reason for Change	Authorised
0.1	Draft	Sept 2020	New policy	Information Governance Steering Group
2	Final	July 2021	No change	Information Governance Steering Group
2.1	Final	Nov 2021	Removal of duplication	Information Governance Steering Group
2.2	Final	Feb 2023	No change	Information Governance Steering Group
3	Final	Feb 2024	Minor updates	Information Governance Steering Group
4	Final	Jan 2025	No change	Information Governance Steering Group
5	Final (this version)	Feb 2026	Minor updates	Information Governance Operational Group

Code Of Conduct for Employees in Respect of Confidentiality

1. Introduction

1.1. The obligation to keep information confidential arises out of legislation and regulation, namely the Data Protection Act 2018 and UK General Data Protection Regulation. This obligation also arises from the common law duty of confidentiality, as well as professional obligations and employment contracts.

1.2. Confidential information is defined as: private or sensitive information generally not known to the public. It is shared under circumstances implying privacy, and includes personal details (names, health), business secrets (trade secrets, financials, customer lists), intellectual property, and technical data.

1.3. Certain categories of information are legally defined as sensitive and should be carefully protected by additional requirements stated in legislation or regulation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

2. Aim and Objectives

2.1. This document has been created to ensure all staff understand their responsibilities in relation to confidentiality as outlined in their contract of employment.

3. Caldicott Principles

3.1. When considering the sharing of personal and/or confidential information, pertaining to patients, all staff should, as a minimum, apply the Caldicott Principles

3.2. The duty to share information can be as important as the duty to protect patient confidentiality.

3.3. Patients and service users have clear expectations of how and why their confidential information is used, and this must be respected.

4. Confidentiality in relation to Patients/Service Users

4.1. Staff are authorised to have access to information they ‘need to know’ to perform their duties.

4.2. Gaining access or attempting to gain access to information that you do not need to see to carry out your work is a breach of confidentiality.

4.3. There are limited certain circumstances under which information can be disclosed without seeking and obtaining consent or where consent is refused. Examples are where there is a legal obligation or there is an overriding public interest, e.g. where child abuse is suspected; or for the protection of vulnerable adults or where failure to disclose would put someone else at risk.

4.4. If a patient does not wish their information to be shared their decision must be respected unless this compromises care. Any decision must be documented in the individual's record.

4.5. If you are in any doubt about the authority or identity of any person whose information has been shared with, advice must be sought from your line manager, Caldicott Guardian, and / or Information Governance.

4.6. All requests for information should be justified, and some may also need to be agreed by a Caldicott Guardian.

5. Abuse of privilege

5.1. It is strictly forbidden for employees to access, view or amend any information relating to themselves, their own family, friends or acquaintances. This is considered an abuse of privilege.

5.2. It is strictly forbidden for employees to view any records out of professional curiosity or interest. This is considered an abuse of privilege.

5.3. It is strictly forbidden to access or utilise records for purposes other than care or administration, where not otherwise appropriately authorised to do so (such as having ethical or explicit consent to research). This is considered an abuse of privilege.

5.4. Staff must not share their login details and passwords with any other person, including other employees, family, friends or acquaintances.

5.5. Staff members must not disclose information to others without appropriate justification.

5.6. All Staff members must remain compliant with mandatory and essential to role data security and protection training.

5.7. Staff must only use systems which are authorised by the Trust.

5.8. Such activities are considered unauthorised and may result in disciplinary action, up to and including dismissal, and referral to processional bodies.

6. Failure to observe this Code of Conduct

6.1. Failure to observe this code of conduct will be regarded as misconduct and:

- Could breach individual's rights and damage the reputation of the Trust
- Could result in disciplinary action being taken against you, up to and including dismissal
- Could lead to your conduct being reported to Professional Regulatory Bodies
- Could lead to legal action being taken against you by others
- Could lead to the organisation being reprimanded and enforcement action (including financial penalty) by the Information Commissioner's Office

7. Maintaining Confidentiality

7.1. In order to maintain confidentiality, all staff must:

- Not talk about individuals in public places or where you can be overheard.
- Not leave any records unattended or in open plan areas.
- Not record any person without their permission (consent) to do so, unless there is an overarching legal basis, such as safeguarding. Please refer to the Body Worn Camera / CCTV Policy for more information.
- Check outgoing correspondence for accuracy, relate to the subject matter and that they are being sent or given to the intended recipient.
- Handle incoming and outgoing information from a clear desk.
- Check intended recipient's email address before sending. Do not assume that the name/email address is correct at all times.
- Only send confidential information that identifies an individual to a Government secure site or via NHSMail/Connect (egress) encryption function.

- Confidentially destroy personal identifiable information in approved confidential waste bins.
- Make sure that any computer screens or other displays of confidential / sensitive information cannot be seen by the others.
- Check all information is filed in the correct record.
- Use safe haven procedures for any information sent / received by fax.