Confidentiality
Code of Conduct

This procedural document supersedes: CORP/ICT 10 v.5 – Confidentiality Code of Conduct

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, <u>it is only valid for 24 hours.</u>**

Executive Sponsor(s):	Ken Anderson – Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Name and title of author/reviewer: (this version)	Roy G Underwood, Data Protection Officer/ Head of Information Governance
Date revised:	March 2023
Approved by (Committee/Group):	Information Governance Group
Date Approved:	22 January 2024
Date issued:	28 February 2024
Next Review Date	July 2026
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 6	March 2023	• Tri-Annual Periodic review with changes to Policy Layout and Monitoring arrangements • Guidance for Switchboard staff • Guidance for Admissions	Roy Underwood
Version 5	July 2020	• Tri-Annual Periodic review with changes to Policy Layout and Monitoring arrangements • Changes to 'current data protection legislation' to reflect GDPR and the DPA 2018 • Change references from Care Groups to Divisions	Roy Underwood
Version 4	April 2015	• Periodic review with changes to Policy Layout and Monitoring arrangements • Change references from CSUs to Care Groups	Roy Underwood
Version 3	May 2012	• Changes to Information Governance Toolkit Standards in v10 (2012) • WPR14452: Your Health Record • Requests by individuals and 3rd Parties to access patient records • Incident Reporting including SI's and the use of STEIS: Strategic Executive Information System • Training • EIA process • Monitoring arrangements	Roy Underwood
Version 2	October 2008	• Changes to Information Governance Toolkit Standard • Changes to reporting authority • Reference to CORP/ICT 20 – Bulk Data Transfer (BDT) Policy • Made reference to the Patient's Charter for England 1996 – page 5 • Reference to Bassetlaw PCT Information Sharing Protocol – page 6	Roy Underwood

Contents

Page No.

1 INTRODUCTION

Much of our work involves us in one way or another, whether on or off of any of the Trust's premises, in having access to confidential and/or sensitive information. Often this can be personal information about staff or patients. We trust our staff to respect these confidences. It is very important. We have produced this Code of Conduct in order to reinforce not only to you, but also to others with whom we do our work, how seriously we treat this matter.

This Code of Conduct also binds our staff to comply with the Statutory Requirements which are;

i) The UK General Data Protection Regulation (UK GDPR) 2021
The Data Protection Act 2018

ii) Copyright, Designs and Patents Act 1988

iii) Computer Misuse Act 1990

iv) Health Records Act 1990

2 PRINCIPLES OF CONFIDENTIALITY

In accordance with the 'current data protection legislation' & the Caldicott Principles, patients have a right to expect that a Doctor, Nurse or other members of our Health Care Teams will not disclose any personal information that is learnt during the course of their professional duties, unless the patient gives their permission or statute permits otherwise. Our guarantee to our patients is detailed in our Trust Privacy Notices which can be found through the Trust Website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

Without assurances about confidentiality, patients may be reluctant to give information which is needed in order to provide good care. For these reasons:

- When you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is 'processed' i.e. manipulated, disposed of, stored, transmitted or received etc;
- When patients provide information about themselves for their immediate and ongoing health care, that our Privacy Notices provide all of the information they need to know about how, why and with whom we have a legitimate basis for processing their personal data[1];

[1] Trust Privacy Notice

- Patients can Opt Out of sharing their information for some purposes. They can find information on the National Opt Out Programme here, and it is for the to opt out, and that it is not for us to opt them out: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

- When you have to disclose confidential information, you should only release as much information as is necessary for the purpose[2]. If it is appropriate to share information gained in the course of your work with other health or social work practitioners for the patients' ongoing healthcare[3]. You must make sure that as far as is reasonable, the information will be kept in strict professional confidence and used only for the purpose for which the information was given (shared);

- If you decide to disclose confidential information, you must be prepared to explain and justify[2] your decision;

- You must abide by these principles in perpetuity (forever!)

3 GUIDANCE ON THE USE AND PROTECTION OF PERSONAL INFORMATION

3.1 People expect that information about them will be treated as confidential.

3.2 'Everyone working for the NHS is under a legal duty to keep your records confidential'. (The Patient's Charter for England 1996).

3.3 Personal information should be anonymised or encrypted wherever possible if it is being moved and it is in electronic format.

3.4 Any personal information held on a computer system is safeguarded by the 'current data protection legislation'. No computerised databases holding personal information should be created or brought into the trust without registration[4] under this legislation. The Trust Senior Information Risk Owner (SIRO) and the Trust Data Protection Officer (DPO) are responsible for maintaining these registrations.

3.5 The unauthorised passing on of personal information by any member of staff is a serious matter, warranting consideration of disciplinary action and possibly risking legal action by others.

3.6 Care should be taken to ensure that unintentional breaches of confidence do not occur, e.g.:

- Do not leave files/computer terminals unattended or insecure

[2] Caldicott et al:1997/2013
[3] UK GDPR Article 9 2(h)
[4] Trust Policy: CORP/ICT 3

- Double check to avoid transmitting information to the wrong person or fax machine[5]
- Do not allow sensitive conversations to be over-heard
- Guard against people seeking information by deception.
- Do not share your Username & Password or Smartcard & PIN
- Log out or Lock your screen down when leaving your desk for any length of time; don't forget to **save** your work **before** you lose it.

3.7 Even if names and addresses are removed, the combination of date of birth and postcode, for example, can allow individuals to be identified.

3.8 Personal information should not be made available to other organisations or individuals without the prior approval of a Senior Manager. In addition, individual **consent** may be required. These measures help to ensure that:

- The Trust complies with 'current data protection legislation'
- Information is held, moved and stored according to specified security standards[6] and used only for agreed purposes[1&7].
- Information in transit in any form complies with the requirements of the Trust's Bulk Data Transfer (BDT) Policy[8] – CORP/ICT 20, where applicable.

3.9 If personally identifiable data is taken off site for proper business purposes, then appropriate measures[9] must be taken to ensure that the data is safeguarded against unauthorised disclosure, loss or destruction.

3.10 Think carefully before you release information to any 3rd Party. This can be especially complicated after a patient's death when relatives sometimes 'need answers'. Always be polite and respectful, and try to direct any enquiries or 'subject access requests[10]' to the Medical Records Casenote Release teams at our main hospital sites.

3.11 Switchboard:

3.12 Admissions:

3.13 Any breach of information security must be reported immediately to the IT Services 'help desk', Head of Information Governance or Caldicott Guardian. Suspected or actual breaches of a delicate or personal or private nature should be directed to the

[5] Safe Haven Guidelines: CORP/ICT 8

[6] NHS Digital: Data Security & Protection Toolkit (DSPT)

[7] SYB ICB (ne: Doncaster and Bassetlaw Clinical Commissioning Groups), Doncaster City Council (ne: DMBC), Notts CC etc. - Information Sharing Protocols

[8] Letters to all Trusts from the NHS Chief Executive of the NHS (December 2007 through May 2008) concerning the carriage and/or transmission of Person Identifying Data (PID)

[9] This usually involves encryption or Pseudonymisation if the information is in electronic format

[10] CORP/REC 3: Procedure for Providing Subject Access to Health Records Under 'current data protection legislation'

Caldicott Guardian or Head of Information Governance in confidence; here the IG Toolkit SIRI reporting tool will be actioned when applicable. Trust Adverse Incident reporting processes should also be completed. Serious Incidents must be reported through STEIS[11] within 24 hours of the occurrence.

3.12 Consideration of the GDPR Articles 46 & 47 must be given when Patient's move abroad outside of the European Economic Community (EEC) where there may be an inadequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Patient's must be fully informed and should normally consent to their data being transferred outside of the EEC. You should always seek guidance from the DPO, the Information Governance Group or the Information Commissioner Website if you need help.

4 TRAINING

Information Governance is now **MANDATORY** for **ALL** Trust staff[12].

All Staff - including Volunteers - must complete their SET Information Governance (IG) training module at least annually, and this will be recorded on their ESR Training Record[13]:

The training requirements of staff will be identified through a training needs analysis. Role specific education will be delivered by the service lead.

5 EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment for All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (see Appendix 1).

[11] STEIS: Strategic Executive Information System

[12] Information Governance Policy: CORP/ICT 9

[13] Some staff, like Volunteers and Locums etc, may not have an ESR training record however, that does not mean that they are excluded from the same levels of training expected of 'employed staff' who have the same or similar access to the Trust's Confidential and Sensitive Information Assets

6 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

Monitoring of this Code of Practice will be through staff fliers.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Staff do not leave files/computer terminals unattended/unsecured Staff double check to avoid transmitting information to the wrong person or fax machine[14] Staff do not allow sensitive conversations to be overheard; beware of the shoulder surfer! Staff guard against people seeking information by deception. Staff Log out or Lock their screen down when leaving their desk for any length of time	The Trust Information Governance, Caldicott & SIRO Support (IGC&SS) Team – Secret Shoppers	One or two areas per month and in line with DSP Toolkit standards	To the IG Committee in line with DSP Toolkit standards

7 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/ICT 8 – Safe Haven Guidelines
CORP/ICT 20 – Bulk Data Transfer Guidelines
CORP/REC 3 - Processing Requests for Access to Health Records Procedure
CORP/EMP 4 – Fair Treatment for All Policy
CORP/EMP 27 – Equality Analysis Policy

8 DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

[14] Safe Haven Guidelines: CORP/ICT 8

APPENDIX 1 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Confidentiality Code of Conduct – CORP/ICT 10 v.6	Digital Transformation Directorate	Roy Underwood	Existing Policy	June 2020

1) Who is responsible for this policy? Digital Transformation Directorate

2) Describe the purpose of the service / function / policy / project/ strategy? Information is treated in Confidence

3) Are there any associated objectives? DSP Toolkit

4) What factors contribute or detract from achieving intended outcomes? Information Governance Training & Education

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? NO

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) Is there any scope for new measures which would promote equality? NO

7) Are any of the following groups adversely affected by the policy? NO

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	**Outcome 2**	**Outcome 3**	**Outcome 4**

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: July 2026

Checked by: **Date:**