Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Confidentiality Code of Conduct

This procedural document supersedes: CORP/ICT 10 v.6 – 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, it is only valid for 24 hours.**

Executive Sponsor(s):	Sam Wilde – Chief Finance Officer
Author/reviewer: (this version)	Roy G Underwood, Data Protection Officer/ Head of Information Governance and Medical Records
Date written/revised:	March 2026
Approved by:	Information Governance and Cyber Group
Date of approval:	27 July 2026
Date issued:	July 2026
Next review date:	February 2029 (Policy valid until July 2029)
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 7	March 2026	• Change mention of 'Staff' to 'Colleague' throughout • Updated advice re access to colleagues own records, or to those of people known to them • Change of name of the IG Committee to the IG and Cyber Group throughout • Change to Executive Sponsor • References to 'EEC' changed to 'EEA' • General language and grammar review	Roy Underwood Rhona McCleery
Version 6	March 2023	• Triennial Periodic review with changes to Policy Layout and Monitoring arrangements • Guidance for Switchboard Colleagues • Guidance for Admissions	Roy Underwood
Version 5	July 2020	• Triennial 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 Colleagues or patients. We trust our Colleagues 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 requires colleagues to comply with the following statutory requirements:

I. The UK General Data Protection Regulation (UK GDPR)
II. The Data Protection Act 2018
III. Copyright, Designs and Patents Act 1988
IV. Computer Misuse Act 1990
V. Access to Health Records Act 1990
VI. Data (Use and Access) Act 2025

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 ;
- 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 Patient 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. 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, you must make sure that, as far as reasonably possible, 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 your decision;
- You must abide by these principles in perpetuity (forever!)

3 GUIDANCE ON THE USE AND PROTECTION OF PERSONAL INFORMATION

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

'Everyone working for the NHS is under a legal duty to keep your records confidential'.

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

Any personal information held on a computer system is safeguarded by the UK GDPR, the Data Protection Act 2018 and other applicable data protection legislation

No computerised databases holding personal information should be created or brought into the Trust without registration under this legislation. The Trust Senior Information Risk Owner (SIRO) and the Trust Data Protection Officer (DPO) are responsible for maintaining these registrations

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

Accessing your own medical records as a member of staff, or accessing the records of those known to you, without following official procedures is a serious violation of data protection laws and professional confidentiality, even if the information is about yourself. In the UK, this is considered unauthorised access under the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR).

- **Key Consequences**
  Disciplinary Action: It will likely result in immediate disciplinary action, which can lead to dismissal for gross misconduct.
  Professional Penalties: If you are a registered professional (e.g., nurse, doctor), you may face action from regulatory bodies like the GMC or NMC, potentially leading to being struck off.
  Criminal Offence: Unlawful obtaining of personal data is a criminal offence, and you could face prosecution by the Information Commissioner's Office (ICO), resulting in a criminal record and fines.
  Audit Trails: IT departments can easily track who accessed records, when, and for what purpose, meaning the access will likely be discovered

- **Why You Cannot "Self-Serve"**
  Even if you have the login credentials (e.g., a Smartcard) to view patient records, **you are only authorised to access records for the direct care of a patient you are currently treating.** Accessing your own record, or those of friends, family, or colleagues, is explicitly not allowed (even if consent is given or perceived).

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
- Double check to avoid transmitting information to the wrong person or fax machine.
- 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 when leaving your desk for any length of time; don't forget to save your work before you lose it

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

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 UK GDPR, the Data Protection Act 2018 and other applicable data protection legislation
- Information is held, moved and stored according to specified security standards and used only for agreed purposes
- Information in transit in any form complies with the requirements of the Trust's Bulk Data Transfer (BDT) Policy (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)) – CORP/ICT 20, where applicable.

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

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' to the Medical Records Casenote Release teams at our main hospital sites.

Any suspected or actual breach of information security must be reported immediately in accordance with the Trust's incident reporting process, including completion of the Trust's adverse incident reporting system where required. Incidents must also be escalated promptly to Information Governance, the Caldicott Guardian and/or the Data Protection Officer, as appropriate. Data security

and protection incidents must be assessed and managed in line with current NHS Data Security and Protection Toolkit requirements and applicable national reporting requirements. Where an incident meets the threshold for external notification, this must be reported within the required timescales.

Consideration of the GDPR Articles 46 & 47 must be given when Patients move abroad outside of the European Economic Area (EEA) 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. Patients must be fully informed and should normally consent to their data being transferred outside of the EEA. You should always seek guidance from the DPO, the Information Governance and Cyber Group or the Information Commissioner https://ico.org.uk/ if you need help.

4 LEARNING/SUPPORT

Information Governance is now MANDATORY for ALL Trust Colleagues.

All Colleagues - including Volunteers - must complete their SET Information Governance and Data Security training module at least annually, and this will be recorded on their ESR Training Record. 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 'Colleagues' who have the same or similar access to the Trust's Confidential and Sensitive Information Assets

The further training requirements of Colleagues 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), the Equality Diversity and Inclusion Policy (CORP/EMP 59) and the Civility, Respect and Resolution Policy (CORP/EMP 58).

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)

6 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

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

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Colleagues do not leave files/computer terminals unattended/unsecured Colleagues double check to avoid transmitting information to the wrong person or fax machine Colleagues do not allow sensitive conversations to be overheard; beware of the shoulder surfer! Colleagues guard against people seeking information by deception. Colleagues 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 and Cyber Group in line with DSP Toolkit standards

7 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/EMP 27 – Equality Analysis Policy
CORP/ICT 03 – Information Management Systems (Registration) Policy
CORP/ICT 08 – Safe Haven Guidelines
CORP/ICT 09 – Information Governance Policy
CORP/ICT 20 – Bulk Data Transfer Guidelines
CORP/REC 03 – Processing Requests for Access to Health Records Procedure

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 (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/

9 REFERENCES

Caldicott et al:1997/2013 The Caldicott Principles - GOV.UK

DBTH Privacy Notice - https://www.dbth.nhs.uk/about-us/our-publications/information-governance/25793-2/

Information Commissioner Website https://ico.org.uk/

NHS Digital: Data Security & Protection Toolkit (DSPT) https://www.dsptoolkit.nhs.uk/

SYB ICB (ne: Doncaster and Bassetlaw Clinical Commissioning Groups), Doncaster City Council (ne: DMBC), Notts CC etc. - Information Sharing Protocols https://www.doncaster.gov.uk/Documents/DocumentView/Stream/Media/Default/AdultSocialCare/DSCP%20and%20DSAB%20MA%20Information%20Sharing%20Agreement%20-%20V2.0%20January%202021%20(003).pdf

The Patient's Charter for England 1996 https://pubmed.ncbi.nlm.nih.gov/8796451/

UK GDPR Article 9 2(h) https://gdpr-info.eu/art-9-gdpr/

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Confidentiality Code of Conduct – CORP/ICT 10 v.7	Digital Transformation Directorate	Roy Underwood	Existing Policy	March 2026

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 (P) 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 – see CORP/EMP 27.

Date for next review: February 2029 (Policy valid until July 2029)

Checked by: Rhona McCleery **Date:** March 2026