Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Data Protection Policy

This procedural document supersedes: CORP/ICT 7 v.7 - Data Protection Policy

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):	Dan Howard – Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Author/reviewer: (this version)	Roy Underwood – Head of Information Governance | Trust Data Protection Officer
Date written/revised:	December 2023
Approved by:	Information Governance Committee
Date of approval:	22nd January 2024
Date issued:	28 February 2024
Next review date:	January 2027
Target audience:	Trust wide

Amendment Form

Date Reviewed	Reason for issue/amendment		~ Authority ~	
			Head of Information Governance	Caldicott Guardian and SIRO
January 2024	Tri annual review ▪ Minor amendments	v.7	Roy Underwood	Dr Tim Noble Dr Nick Mallaband and Dan Howard
July 2020	▪ Minor amendment to access rights for staff	v.6	Roy Underwood	Dr Tim Noble and Ken Anderson
Sept 2018	Tri annual review ▪ Amended in line with GDPR and the Data Protection Act (DPA) 2018 ▪ SIRI reporting in line with DPA under the Data Security and Protection Toolkit Incident Reporting Tool	v.5	Roy Underwood	Mr Sewa Singh and Simon Marsh
October 2016	Tri annual review ▪ The original DoH guidance has now been withdrawn in favour of advice from NHS Digital ▪ The revised NHS Digital Records Management Code of Practice or Health & Social Care was launched in July 2016. It includes: - The Code and the Retention Schedule - The Retention Schedule only ▪ *The EU General Data Protection Regulation 2016 may impact on this policy* ▪ Use of the Internet and eMail Policy: CORP/ICT 26 is now an IT Services Policy	v.4	Roy Underwood	Mr Sewa Singh and Simon Marsh
October 2013	Reviewed without change - changes to policy format & layout.	v.3	Roy Underwood	Mr Sewa Singh and David Pratt
April 2010	▪ Policy re-write for NHSLA Compliance layout & content ▪ Additional information about Records management policy – page 4 ▪ Separation of Caldicott Guardian and SIRO responsibilities – page 5 ▪ FOI provides subject access to unstructured data available through DPA ▪ Audit & Monitoring rationale – page 10	v.2	Roy Underwood	Dr Robin Bolton and Kevin Turner
May 2007	Reviewed without change. IG Minute 07/227 21/5/2007 refers	v.1	Roy Underwood	Dr Emyr W Jones
2May 2006	Reviewed without change -minor changes to policy layout.	v.1	Roy Underwood	Dr Emyr W Jones
May 2004	Implementation	v.1	Roy Underwood	Dr Emyr W Jones

Contents

Page No.

The information and guidelines within this policy are important and apply to the entire Trust. This policy does **not** cover GP records but covers the records held and processed by staff employed by Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust. A Code of Conduct in respect of Confidentiality is issued under separate cover[1].

1 INTRODUCTION

Like all NHS establishments, Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust ("the Trust") holds and processes information about its employees, patients and other individuals for various purposes (for example, the effective provision of healthcare services or to operate the payroll and to enable correspondence and communications). To comply with current data protection legislation (the UK GDPR and the Data Protection Act 2018) vis-a-vis their assertions and principles, that information must be collected and used fairly, stored safely and not disclosed to any unauthorised persons. The legislation applies to both manual and electronically held data.

2 PURPOSE

This policy covers records held and processed by the Trust. The Trust is responsible for its own records under current data protection legislation, and it has submitted and maintains an annual notification to the Information Commissioner - Registry No. Z5372151.

The lawful and correct treatment of personal information is vital to successful operations, and to maintaining confidence within the Trust and the individuals with whom it deals. Therefore, the Trust will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held[2];
- ensure that the rights of people about whom information is held can be fully exercised under current data protection legislation. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information.);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

[1] CORP/ICT 10 Confidentiality - Code of Conduct

[2] NHSx: Records Management Code of Practice & Retention Schedule 2021: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

3 NOTIFICATION TO THE INFORMATION COMMISSIONER AND OUR DUTIES UNDER THE DATA PROTECTION ACT 2018

The Trust has an obligation as a Data Controller to notify the Information Commissioner (formerly called the Data Protection Registrar) of the purposes for which it processes personal data. Notification monitoring within the Trust is carried out by the Head of Information. Individual data subjects can obtain full details of the Trust's data protection registration/notification with the Information Commissioner from the Information Governance Manager or from the Information Commissioner's website (https://ico.org.uk).

Serious Incidents Requiring Investigation (SIRIs) will also be formally reported to the ICO through the Data Security and Protection Toolkit Incident Reporting Tool, complementary to the usual Trust SI reporting processes.

3.1 Data Protection Principles

The Trust, as a Data Controller, must comply with the Data Protection Principles that are set out in current data protection legislation. In summary these state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary for those purposes;
- Be processed in accordance with the data subject's rights under GDPR and the 2018 Act;
- Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction;
- Not be transferred to a country outside the European Economic Area, unless that country or territory has equivalent levels of protection for personal data.

3.2 Processing

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data;

(b) retrieval, consultation or use of the information or data;

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data;

(e) viewing personal data, even where no changes are made to the data.

3.3 Personal Data Sources

- Patient related
- Non-patient related
- Electronic records
- Manual records
- Post and fax transmissions
- Photographs - including digital images from Cameras and Mobile Phones[3]
- Video & Transparencies
- Films and X-ray
- The spoken word

3.4 Sensitive Personal Data

The Trust may from time to time process "special category data" relating to staff, patients and other individuals as in the UK GDPR Article 9 and in the DPA S.35 (8) and S.48

3.5 Consent

Certain types of personal data may be processed for particular purposes without the consent of individual data subjects, relying - post 25/5/2018 - on a 'legal basis' for processing as in the UK GDPR Art 9 2(h). However, it is the Trust's policy to explain its data processing activity whenever practicable to individual data subjects. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The Trust will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law. The Trust will normally seek **the explicit consent** of the individual in question, where their personal data may be used for non-treatment purposes such as Research etc. Here the National Data Opt-out Programme may also be used by members of the public to hold their personal choice in these matters. The DBTH – through the Information Services Department - will always check against the National Register to ensure that the rights of those persons who have opted out are observed.

3.6 Rights of Access to Personal Data

Staff, patients and other individuals have the right under current data protection legislation to request access through a subject access request (SAR) any personal data that is being held about them.

An individual who wishes to exercise his/her right of access is asked to formally request this information as follows:

- For access to personal medical records - apply, in writing, to the Casenote Release Team: dbth.casenoterelease@nhs.net following which an official application form will be issued.

[3] The use (on-site) of Mobile Phones is strictly controlled through the Mobile Phone Policy

- For personal 'staff' access to personnel records - members of staff should apply through their Line Manager who should comply with the guidance and policy statements in CORP/ICT 30: Data Subject Access Request (DSAR) Policy.

Any inaccuracies in data disclosed in this way should be communicated immediately to the responsible Medical Records Manager or their Line Manager, who will take appropriate steps to make the necessary amendments.

Requests made under current data protection legislation will be:

- Free of charge, excepting where the request is 'manifestly unreasonable'[4] or when requesting a copy of any records previously provided for a SAR actioned on or after the 25/5/2018.

- Any fees due will be agreed, and based on the amount of copying necessary, by relevant managers at the time of the request.

The Trust will respond to the request for access to personal data within 1 month (30 days) (including bank holidays and weekends) of the request.

Staff have **no right of access** – at work - to:

- their own medical and confidential records however, they can request copy via the Trust SAR process as described above
- medical and confidential records of their own family, relatives, friends or acquaintances, unless they are directly involved in the patient's clinical care, or with the employee's administration on behalf of the Trust[5].

Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action by the Trust.

3.7 Disclosure outside of the European Economic Area (EEA)

The Trust or its contracted Data Processors may, from time to time, need to process personal data in countries or territories outside of the EEA in accordance with purposes made known to individual data subjects through its Privacy Notices. For example, the names and contact details of Trust members of staff on a website may constitute a transfer of personal data world-wide. If an individual wishes to raise an objection to this disclosure, then written notice should be given to the Trust's Communications Manager.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures are taken, be processed, or transferred outside the EEA unless UK GDPR compliant agreements are in place with individual Data Processors.

[4] Awaiting guidance from the ICO on what can be considered to be 'manifestly unreasonable'

[55] Where staff have a legal basis in that it is either clinically appropriate (GDPR Art 9 2(h)) or as a result of an Admin process (GDPR Art 6 1(e))

4 STAFF ACCOUNTABILITY AND RESPONSIBILITIES

4.1 Trust Staff with Data Protection Responsibilities

All queries about this Trust policy should be directed to Head of Information Governance who reports directly to the Trust's Senior Information Risk Owner (SIRO)/Chief Information Officer. Information Asset Owners (IAOs) are directly responsible to the Trust's SIRO for the safe and effective control and management of the Personal Information Assets that they are registered for.

All requests for access to personal data relating to patient records should be addressed to the Casenote Release Team: dbth.casenoterelease@nhs.net.

All requests for access to staff personnel files should be addressed to the line manager who holds a particular individual member of staff's records.

(see also point 3.6: Right to Access Personal Data for more details).

4.2 Responsibilities of Individual Users

All employees of the Trust who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with:

- the requirements of Current data protection legislation (especially the Data Protection Principles)
- the Trust's Information Asset Registration Policy (CORP/ICT 3), and any procedures and guidelines which may be issued from time to time.

Consideration of the UK GDPR in parallel the principles of the 2018 Act should be made:

1. when using an existing computer system to process personal data for a new purpose - it may be necessary to notify an amendment to an existing registration to the Trust's Information Asset Registration Policy;

2. when creating a new manual filing system containing personal data;

3. when using an existing manual filing system containing personal data for a new purpose.

4.3 Accuracy of Data (Data Quality)

All staff are responsible for:

- checking that any personal information they provide to the Trust in connection with their employment is accurate and up to date e.g. change of address/contact details (personal phone numbers and email addresses). The Trust cannot be held responsible for any errors unless the member of staff has informed the Trust about them.
- In supplying their contact details, members of staff agree to the trust using them in order to manage their contract and to contact them, unless they are advised to the contrary.
- checking that any patient, staff, or other individual's information that they handle is as accurate and up to date as possible[6].

4.4 Data Security and Disclosure

All staff within the Trust are responsible for ensuring that:

- Any personal data that they hold is kept secure[7], relative to the security level of the data.
- Personal data are not disclosed either orally or in writing or otherwise (eMail, Text Messaging, or any other Social Media Platform) to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. Any inappropriate disclosure must be reported to the trust DPO: dbth.dpo@nhs.net as soon as is practically possible and in any case within 48 hours to enable the DPO to carry out their statutory duties within 72 hours when it is appropriate.

Personal data must be kept secure at all times, and examples of how this may be done will include:

- keeping the data locked in a filing cabinet, drawer or room; or
- if the data is computerised, ensuring that the data is kept safe as detailed in trust policy CORP/ICT 2 – Information Management and Technology (IM&T) Security Policy

[6] Data Quality Policy CORP/ICT 23
[7] Data Protection Act 2018

5 CCTV

A number of CCTV cameras are present on the Trust's Hospital sites. The notified purposes of the CCTV Systems are:

- Preventing and detecting crime.
- Apprehending and prosecuting offenders.
- Protecting public safety.
- To assist with security for staff, patients, other individuals and their property, as part of the Doncaster Crime and Disorder Partnership with the Police, and in accordance with the Trust's 'notification' to the Information Commissioner. If you have any queries regarding the operation of or access to the CCTV system, please speak to the Trust Security Manager.

6 E-MAIL

It is permissible and appropriate for the Trust to keep appropriate records of internal communications, provided such records comply with current data protection legislation, the Freedom of Information Act 2000, and the Trust's Information Records Management Policy[8].

The appropriate use of E-Mail in the proper functioning of the Trust, and the limitations of use can be found in the Trust's Internet and E-Mail Policy[9].

However, all Trust staff need to be aware that:

- Current data protection legislation applies to E-Mails which contain personal data about individuals which are sent or received by Trust staff;
- subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to E-Mails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the Trust to locate the personal data in the E-Mails; and that that search would satisfy 'the personal data test' described in Durant v Financial Services Agency et al;
- the legislation applies to all E-Mails from and to members of the Trust which are sent and received for Trust purposes;
- E-Mails, like other Trust correspondence, need to be managed and archived for as long as necessary in order to meet local and corporate business needs.

7 RETENTION OF DATA

The Trust will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which they will be destroyed. This will be done in

[8] CORP/ICT 14 CORP/ICT 14 – Information Records Management – Code of Practice
[9] CORP/ICT 27 – Email and Internal Communications Policy

accordance with the retention periods detailed in the Trust's Information Records Management[8] and Medical Records Retention and Destruction Policies[10]

8 MONITORING (THE EFFECTIVENESS OF THE POLICY)

Monitoring the effectiveness of the policy will be achieved through periodic Audit with the results going to the Information Governance Group to the Audit and Non Clinical Risk sub Committee and the Board of Directors.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Staff Awareness Surveys	Head of Information Governance	Annually	DSPT Assertion NDG 3

9 DEFINITIONS

CCTV – Closed Circuit Television
DPA – The Data Protection Act 2018 (current data protection legislation)
HSC – Health Service Circular
UK GDPR – United Kingdom General Data Protection Regulation (current data protection legislation)

10 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).

[10] CORP/REC 8 - Legal Retention and Destruction of Hospital Patient Medical Records

11 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

Processing Requests for Access to Health Records Procedure - CORP/REC 3
Information Management Systems (Registration) Policy - CORP/ICT 3
Information Management and Technology (IM&T) Security Policy – CORP/ICT 2
Equality Analysis Policy - CORP/EMP 27
Fair Treatment for All Policy – CORP/EMP 4
Data Subject Access Request (DSAR) Policy – CORP/ICT 30

12 REFERENCES

None.

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
Data Protection Policy CORP/ICT 7 v.7	Digital Transformation/IGC&SS	Roy Underwood	Existing	January 2024

1) Who is responsible for this policy? Name of Division/Directorate: SIRO/CIO's Office

2) Describe the purpose of the service / function / policy / project/ strategy? Trust-wide Information Governance Policy

3) Are there any associated objectives? Compliance with GDPR, the Data Protection Act 2018 and Confidentiality Legislation

4) What factors contribute or detract from achieving intended outcomes?

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?

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: January 2027

Checked by: **Date:**