The Robert Jones and Agnes Hunt Orthopaedic Hospital

NHS Foundation Trust

Title:	Data Protection Policy		
Unique Identifier:	POL003	**Document Type:**	Policy
Version Number:	5.0	**Status:**	Approved
Responsible Director:	Deputy Chief Executive/Director of Nursing (Caldicott Guardian)		
Author:	Information Governance Officer/Data Protection Lead		
Scope:	Trust Wide		
Replaces:	Version 4.0		
To be Read in Conjunction with the Following Documents: (list related policies)	• Confidentiality Code of Conduct • Records Management Policies & Procedures • Subject Access Request Policy		
Keywords:	Data Protection		

Considered By Executive Owner:	Deputy Chief Executive/ Director of Nursing	**Date Considered:**	20/11/2018
Endorsed By:	Deputy Chief Executive/ Director of Nursing	**Date Endorsed:**	20/11/2018
Approved By:	Information Governance Committee	**Date Approved:**	17/12/2018
Issue Date:	17/12/2018	**Review Date:**	20/11/2021
Security Level:	**Open Access** ✓	**Restricted**	**Confidential**

DATA PROTECTION POLICY

CONTENTS

Key Points

- All roles and responsibilities for implementation of the Data Protection Act are clearly defined
- Requirement to accurately obtain consent before processing data
- Requirement to record Information accurately
- Holding information securely and confidentially

1. INTRODUCTION

The Robert Jones and Agnes Hunt Orthopaedic Hospital NHS Foundation Trust have a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the NHS Executive and other advisory groups to the NHS and professional bodies.

2. BACKGROUND

The General Data Protection Regulation (GDPR) was published by theEuropean Union (EU) and this forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018) which replaces DPA1998. The new GDPR and DPA came into force on the 25 May 2018.

The data protection legislation applies to living individuals and gives those individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing.

Under the data protection legislation individuals have a right to make requests to the Trust regarding the use of their information; this is called a Subject Access Request (SAR). The Trust, as a Data Controller, must respond to these requests" without undue delay and at the latest within one month of receipt".

3. PURPOSE

The Trust has a responsibility under the Data Protection Act 2018 to hold, obtain, record, use and store all personal identifiable data in a secure and confidential manner and in accordance with the purpose stated within its Data Protection Notification.

The Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Trust, who may be held personally accountable for any breaches of information security for which they may be held responsible.

4. SCOPE

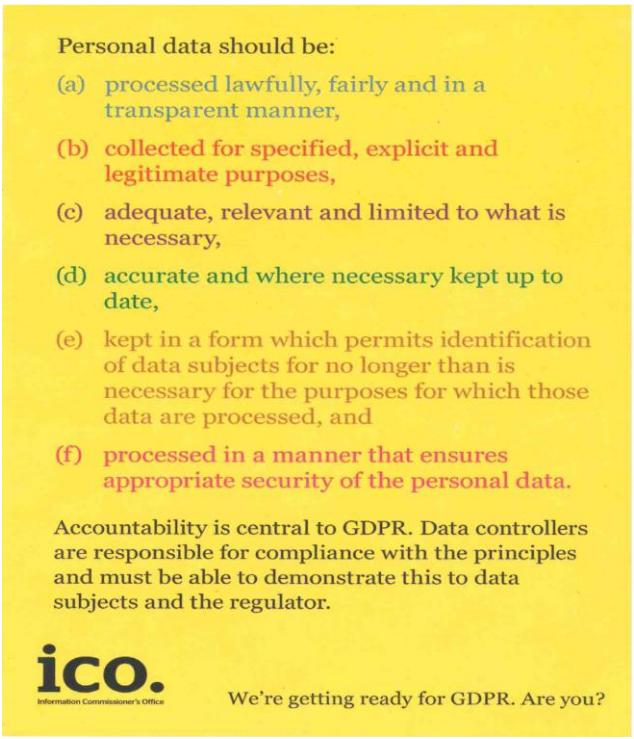
This policy covers the processing of personal data (i.e. information about living individuals) whose use is controlled by the Trust and defined in the Trust's Data Protection Notification.

It applies to all staff (including new starters, locum, temporary, student and contract staff) who process data on behalf of the Trust. 'Personal data' describes both computer and manual records.

Any breach of the Act may result in formal litigation action against the Trust or the individual, by the Information Commissioners Office.

5. MAIN FEATURES OF THE ACT

All data covered by the Act must be handled in accordance with the six Data Protection Principles (see yellow postcard below)



.

Every organisation that processes personal information must submit a notification to the Information Commissioner, unless they are exempt. The notification includes a description of the data subjects about whom personal information is held, the purpose(s) for which it is held, the classes of data, a list of the recipients of that data i.e. who that data will be shared with. Failure to notify constitutes an offence under the act.

The Information Commissioner (ICO) is responsible for policing that Act and issues Information and Enforcement Notices to organisations where they are not complying with the requirements of the Act. It also has the ability to prosecute those who commit offences under the Act.

An Information Tribunal (a separate body) hears appeals against decisions made by the Information Commissioner under the Act.

The Trust shall comply with the following legislation and guidance as appropriate:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (DPA 2018)
- The Caldicott Report (1997)
- Human Rights Act (1998)
- The Computer Misuse Act (1990)
- NHS Confidentiality Code of Practice (2003)
- Common Law Duty of Confidentiality
- Administrative Law
- The NHS Care Record Guarantee

6. INDIVIDUAL RIGHTS

In accordance with the data protection legislation individuals have the following rights:

Informed: Individuals have the right to be **informed** about the collection and use of their personal data. This is a key transparency requirement under the law and the Trust is required to publish a Privacy Notice to explain this

.

Access: Individuals have the right to access their personal data

.

Rectification: The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete

.

Erasure: The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.

Restriction: Individuals have the right to request the restriction or suppression of their personal data.

Data Portability: Allows individuals to obtain and reuse their personal data for their own purposes across different services.

Object: The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.

Automated Decision Making: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Not all the individual rights are absolute – it is the right to request that is absolute.

7. ROLES AND RESPONSIBILITIES

a. Chief Executive

The Trusts Chief Executive has overall responsibility for compliance with the Data Protection Act. Operational responsibility for Data Protection is delegated to the Caldicott Guardian and the Trust Data Protection Officer

b. Caldicott Guardian

The Caldicott Guardian, under delegated authority from the Chief Executive, will oversee compliance with the Data Protection Act, and the development of appropriate policy and procedure. The Caldicott Guardian will be advised by the Data Protection Officer and supported by the Information Governance Committee.

c. Senior Information Risk Owner (SIRO)

The Trust SIRO is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards and will work closely with the Caldicott Guardian and Trust Data Protection Officer

d. Data Protection Officer (DPO) (This role will be carried out by the Trust Secretary)

Will be responsible for assisting with monitoring internal compliance of our data protection obligations. They will inform and advise on data protection, including Data Protection Impact Assessments(DPIAs) and act as a contact point for data subjects and the supervisory authority.

e. Data Protection Lead

The Trust Data Protection Lead in conjunction with the DPO is responsible for the developing and monitoring of relevant policy and procedure, ensuring training is provided where required and providing advice on all related Data Protection matters to the Trust and its employees. The Data Protection Lead will also ensure that the Trust re-submits an annual Data Protection Notification and fee to the Information Commissioners Office.

f. Information Governance Committee

The Information Governance Committee will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act and will be responsible for discussing and resolving any Data Protection and Confidentiality issues which may arise.

g. All staff and Executive Directors

All staff will ensure that:

- Personal information is treated in a confidential manner in accordance with this and associated policies;
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose. (This consent should be recorded and signed by the data subject);
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information;
- Personal information is recorded accurately and is kept up to date;
- They create and maintain their own records in accordance with the Trust's Record Management Policies and Procedures and any associated policies and procedures to facilitate easy location should they be required;
- They refer any potential or actual Subject Access Requests to the appropriate member of staff as outlined in the Trust's Subject Access Request Policy;
- They raise actual or potential breaches of the Data Protection Act with their Line Manager, the Trust's Data Protection Lead and Caldicott Guardian and report incidents on the Trust's DATIX system;

It is the responsibility of all staff to ensure that they comply with the requirements of this policy and associated policies or procedures. Failure to do so may result in disciplinary action.

h. Contractors & Employment Agencies

Where contractors or employment agencies are used, the contracts between the Trust and these third parties should contain clauses to ensure that the contract states that staff are bound by the same code of behaviour as Trust staff.

i. Volunteers

All Volunteers are bound by the same code of behaviour as Trust Staff.

j. Heads of Profession/ Departmental Managers/ Lead Nurses/ Team Leaders

All Heads of Profession, Departmental Managers, Lead Nurses and Team leaders should be fully aware of their own responsibilities in regards to the Data Protection Act.

They will ensure that:

- All staff for whom they are responsible are provided with appropriate training with regard to the requirements of the Act and their responsibilities under it;
- Information is created and stored in line with the Trust's Records Management Policies/ Procedures to facilitate easy location should it be required;
- Personal information is only used for the purposes specified within the Trust's Data Protection Notification;
- Information is handled in a secure and confidential manner;
- The IG Team is notified of all data held, processed and transferred within their area, in order that the Trust can ensure that the Data Protection Notification covers their use;

- Records are retained in accordance with the Trust's Procedures for Retention, archiving and destruction;
- They comply with Data Protection Audits as and when required.

8. DEFINITIONS

Personal Data
Data which is related to a living individual who can be identified either from those data or from those data in conjunction with any other data which is, or is likely to come into the possession of the Data Controller and includes any expression of opinion and any indication of the intention of the Data Controller or ant other person in respect of the individual.

Personal Data held by the Trust and therefore subject to the provisions of the Act includes information about patients, staff, contractors and volunteers.

Data Subject
The Individual to which the data relates, e.g. patients, staff

Data Controller

An individual or organisation who, either alone, jointly or in common with other persons, decides the purposes for which personal data are, or will be processed and the way in which that data are or will be processed.

Sensitive Data

Sensitive/confidential data under the Act includes, but is not restricted to:

- Demographics e.g. Name, Address, date of birth;
- Information about a person's racial or ethnic origin;
- Political opinions;
- Gender;
- Religion and belief;
- Membership of a trade union;
- Physical or mental health;
- Sexual life;
- Criminal convictions or charges.

The Trust may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety, or comply with the requirements of other legislation.

9. RECORDS MANAGEMENT

Good records management practice plays a pivotal role in ensuring that the Trust is able to meet its obligations to provide information in a timely and effective manner in order to meet the requirements of the Act. It is necessary to ensure that robust records management practices are in place which are understood and implemented by all staff dealing with records within the Trust.

It is the responsibility of all staff to ensure that they are familiar with the policies/ procedures relating to records management within the Trust.

10. CONSENT

If consent is the chosen legal basis for processing, the Trust will take all reasonable steps to ensure that patients, staff, volunteers, contractors are informed of the reasons the Trust requires information from them, how that information will be used and who it will be shared with, this will enable the Data Subject to give informed consent to the Trust handling their data.

Should the Trust wish to use personal data for any purpose other than that specified when it was originally obtained, the Data Subject's explicit consent should be obtained prior to using the data in the new way.

Should the Trust wish to share personal data with anyone other than those recipients specified at the time the data was originally obtained, the Data Subject's explicit consent should be obtained prior to sharing that data, failure to do so could result in a breach of confidentiality.

Failure to obtain explicit consent to either use or share personal data in ways other than those specified when the data was obtained could result in a breach of the First Data Protection Principle, i.e. that "Personal data shall be processed fairly and lawfully".

Information may be exchanged for the purposes of which consent was obtained for example clinicians may share information where they are involved in direct patient care.

11. SYSTEMS CONTAINING PERSONAL INFORMATION

A database is any collection of personal information that can be processed by automated means, these could include:

- Patient/ personal records (names and addresses etc) for appointments;
- Patient/ Personal information used for research e.g. where only NHS Number (or other personal identifier may be allocated) and clinical details may be held. This may be a simple Excel Spreadsheet;
- Patient/ personal details used for prescribing drugs;
- Staff records held on an Excel Spreadsheet to monitor annual leave and sickness;
- Staff personal details used for monitoring training course attendance.

It is important that data collected from individuals is both accurate and complete and is justified for the purpose for which it is being collected.

All new system developments / amendments to new systems to be carried out should have appropriate Data Protection Impact Assessments completed as per the Trust's Data Protection Impact Assessment Procedure and should be notified to the Trust's Data Protection Officer

12. RETENTION AND DISPOSAL OF INFORMATION

All records should be retained and disposed of in accordance with the Trust's Corporate Records Management Policy.

13. ACCURACY/ DATA QUALITY

It is the right under the Data Protection Act 2018 of any living individual about whom personal information is held, for that information to be accurate, relevant and up to date. In order to ensure compliance with the Act, the trust will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the Data Subject. The Trust will also take steps to identify discrepancies between electronic and paper based records through the use of internal data quality audits.

All staff must ensure that patient personal information is checked and kept up to date on a regular basis by checking it with the patient when they attend for appointments in order that the information held can be validated.

Staff information should be checked for accuracy on a regular basis by the line manager.

14. COMPLAINTS

The Data Protection Act 2018 gives individuals the right to complain if they feel their data has been misused or that the organisation holding it has not kept it secure.

Should the complainant remain dissatisfied with the outcome of their complaint to the Trust once the complaints procedure has been exhausted, a complaint can be made to the Information Commissioner's Office (ICO) who will then investigate the complaint and take action where necessary.

15. SECURITY AND CONFIDENTIALITY

All staff must ensure that information relating to identifiable individuals is kept secure and confidential at all times.

The Trust will ensure that its various holdings of personal data are properly secured from loss or corruption and that no un-authorised disclosures of personal data are made.

The Trust shall ensure that all members of staff are aware of the existence of the Trust's Code of Conduct for employees in respect of confidentiality and that they adhere to its provisions.

16. TRAINING

Trust staff will be informed of their responsibilities under the Data Protection Act through the normal communication mechanisms within the Trust, including Induction and Statutory training.

Heads of Profession, Departmental Managers and Team Leaders in line with their responsibilities detailed in section 6.8 will be responsible for ensuring their staff attend training and are aware of their responsibilities under the Act.

17. MONITORING AND AUDIT

This policy and associated procedures will be monitored by the Information Governance Committee and the Data Security and Protection Toolkit. An annual compliance check programme has been devised that incorporates aspects of the Data Protection Act and its principles and the effectiveness of this Policy will be monitored through these checks. The structure of the compliance checks will be reviewed regularly to ensure differing aspects of the Data Protection Act and its principles are covered during the checks.

If the audit identifies any deficiencies, an action plan will be produced to reduce them. The findings of the audits and any subsequent recommendations will be presented to the Information Governance Committee for review.

18. OFFENCES UNDER THE ACT

It is an offence to process personal data without notification, or failure to notify the Commissioner of changes to the notifications register entry.

It is an offence for a person, knowingly or recklessly, without the consent of the Data Controller to obtain, disclose or procure personal data or the information contained in personal data unless the person can show:

- It was necessary to prevent or detect crime;
- It was required or authorised by law;
- They acted in the reasonable belief that they has a legal right to do so;
- The Data Controller would have consented to it if they had known;
- In the particular circumstances it was justified as being in the public interest.

19. REVIEW

This policy will be reviewed every three years, or earlier if appropriate, to take into account any changes to legislation that may occur, and/ or guidance from the Department of Health, the NHS Executive and/ or the Information Commissioner.

Amendments History

Record of Amendments to: Data Protection Policy Version 4.1				
				Date *Date approval for amendment given*
Section number *Paragraph(s) amended*	**Amendment** *Section amended with changes shown in bold italics*	**Deletion** *Section which has been removed*	**Addition** *Section which has been added*	**Reason** *Why has the document been changed*
Standard Cover Sheet	***Director of Nursing***	**Interim**		**August 2013 Change to role**
Standard Cover Sheet	***Approved***	**Draft**		**August 2013 Update**
Scope 4.2	***It applies to all staff*** **(including new starters, locum, temporary, student and contract staff) who process data on behalf of the Trust. *'Personal data' describes both computer and manual records.***	**or agents of the Trust**	**(including new starters, locum, temporary, student and contract staff)**	**May 2014 To strengthen the Policy to ensure it captures temporary(bank) staff in its scope**
19.2 - Associated Legislation and Guidance		**NHS Code of Practice: Records Management April 2006**	**Records Management Code of Practice For Health and Social Care 2016**	**March 2017**
Policy updated October 2018 for GDPR and DSPT compliance			**All relevant legislation and guidance**	**October 2018**