The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

DATA PROTECTION POLICY

Primary Intranet Location	Version Number	Next Review Year	Next Review Month
Information Management & Governance	4	2021	September

Current Author	Phil Cottis
Author's Job Title	Head of Health Records and IG
Department	Business Support
Ratifying Committee	Information Governance Committee
Ratified Date	13th September 2018
Owner	Jon Wade
Owner's Job Title	Chief Operating Officer

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet

Related Policies	Access to Health Records Policy & Procedure Confidentiality Code of Conduct Corporate Records Procedure Data Encryption – Security of Email and Removable Media Policy Freedom of Information Policy Guide to the Safe Use of Personal Mobile Media Devices Health Records Management Policy Information Governance Policy Information Lifecycle and Records Management Policy Information Risk Policy Data Security Policy Internet and Email Acceptable Use Policy Mobile Computing Policy Safe Haven Policy & Procedure

Stakeholders	Information Governance Committee Trust Executive Board

Version	Date	Author	Author's Job Title	Changes
V1	September 2010	Nic McCullagh	Information Governance Manager	
V2	September 2012	Phil Cottis	IG & RA Manager	Review and new format
V3	September 2015	Phil Cottis	IG & RA Manager	Review and new format
V3.1	April 2018	Phil Cottis	Head of Health Records & IG	GDPR compliance
V4	September 2018	Phil Cottis	Head of Health Records & IG	Review. Data Protection Officer responsibilities under GDPR

Short Description
Data protection is a large and complex issue which affects the whole organisation and should be understood by every member of staff, not just one delegated person. This policy sets out how the Trust aims to meet its legal obligations and NHS requirements concerning the security and confidentiality of personal confidential data.

Key words
Breach of confidentiality, Data protection, Data subject access, Personal confidential data, Subject access request.

CONTENTS

DATA PROTECTION POLICY

1 INTRODUCTION

1.1 This policy sets out in broad terms the duties placed upon the Trust by the common law duty of confidence, the Data Protection Act 2018 (DPA), the General Data Protection Regulation and guidance provided by the Information Commissioner's Office, Department of Health and other relevant bodies.

1.2 Penalties can be imposed on the Trust and / or staff for non-compliance with relevant legislation. Therefore this policy applies to all staff, and anyone working on behalf of the Trust.

1.3 The DPA is closely linked with the Freedom of Information Act and the Human Rights Act. The focus of the DPA is on promoting the rights of living individuals in respect of their privacy and the right to security and confidentiality of their data. It applies to all personal confidential data, whether held manually or electronically. The responsibility to maintain the confidentiality of that data resides with the Trust, even if an agent or subcontractor processes that data.

1.4 The DPA does not guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal confidential data.

1.5 The DPA also allows people to find out what information is held about them by making a Subject Access Request. These are handled by the Legal Services Department. For more information about Subject Access Requests, please refer to the 'Access to Health Records Policy & Procedure' available on the intranet.

1.6 The Trust is obliged by law to register all processing activities with the Information Commissioner's Office on an annual basis and failure to comply with this requirement is a criminal offence.

2 PURPOSE

2.1 Data protection is a large and complex issue which affects the whole organisation and should be understood by every member of staff, not just one delegated person. This policy sets out how the Trust aims to meet its legal obligations and NHS requirements concerning the security and confidentiality of personal confidential data. Staff adhering to this policy and other related documents, as described in the following sections, should be in compliance with the DPA.

2.2 For the purpose of this policy, 'staff' is used as a convenience to refer to all staff regardless of occupation, including but not restricted to permanent, fixed-term, contractors, bank, agency, temporary, honorary, visiting, voluntary and students.

2.3 This policy relates to all personal confidential data, both clinical and non-clinical, that are received, transferred or communicated both within and outside the Trust.

2.4 Person identifiable information may be in any form including, but not restricted to, the following:

- Paper records or documents;
- Computer records or printouts;
- Fax messages;
- Telephone conversations;
- emails and attachments; and
- CDs, memory sticks or other portable media.

3 DEFINITIONS

3.1 **Breach of Confidentiality**
A breach of confidentiality is the unauthorized disclosure of personal confidential data provided in confidence.

3.2 **Data Subject**
A data subject means an individual who is the subject of personal data and must be a living individual. Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects. The data subject need not be a United Kingdom national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.

3.3 **Personal Confidential Data**
Personal confidential data can be anything that relates to patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, BlackBerrys, mobile telephones) or even passed by word of mouth.

Key personal confidential data includes:

- Patient's name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients;
- NHS number and local patient identifiable codes;
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.4 **Sensitive Personal Data**
Sensitive Personal Data means personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health conditions;

- Sexual life; and
- The commission or alleged commission of any offence.

4 RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive is the accounting officer responsible for the management of the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to the Trust being able to supply a first class confidential service that provides the highest quality patient care. The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 Senior Information Risk Owner (SIRO)

An Executive Director has been appointed as the Senior Information Risk Owner (SIRO) with overall responsibility for information governance, of which confidentiality is a key part.

4.3 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.4 Data Protection Officer (Head of Health Records and IG)

The Data Protection Officer role includes:

- The DPO's tasks are very clearly delineated in the GDPR Article 39, to:
- Inform and advise the Data Controller or Data Processor and the employees who carry out processing of their Data Protection obligations.
- Monitor Data Protection compliance.
- Assign responsibilities, awareness-raising and training of staff involved in processing operations.
- Undertake internal audits of Data Protection.
- Provide advice on the need and completion of Data Protection Impact Assessments.
- Cooperate with the ICO and act as the contact point for any issues relating to processing
- Undertake or advise on the potential risk of processing activities.
- Under the GDPR, DPOs have many rights in addition to their responsibilities; they:
- May insist upon resources to fulfil their job functions and for their own ongoing training.
- Must have access to the company's Data Processing personnel and operations,
- Have significant independence in the performance of their roles,

- Have a reporting line 'to the highest management level' of the organisation.

4.5 **Head of Health Records & IG**

The Head of Health Records & IG is responsible for advising on strategic direction, the development of policy and guidance for the Trust, and also operational support to the Trust.

4.6 **Legal Services Department**

The Legal Services department is responsible for the day-to-day management of Subject Access Requests, to ensure they are handled in accordance with Trust policy and legal requirements. Quarterly reports on compliance with standards are provided to the Information Governance (IG) Committee.

4.7 **Trust Management**

Directors/Heads of Department/Departmental Managers etc will be responsible for ensuring that staff for whom they are responsible are aware of their responsibilities with regard to confidentiality of information, ensuring that staff receive appropriate confidentiality training.

They will be responsible for ensuring that their staff are fully aware of the mechanisms for reporting actual or potential confidentiality breaches within the Trust.

4.8 **All Staff**

All employees and anyone working on behalf of the Trust must adhere to this policy to support the reputation of the Trust and where relevant of their profession. Employees must make sure that they conduct themselves online in the same manner that would be expected of them in any other situation.

5 OVERVIEW

5.1 The DPA regulates when and how a data subject's personal confidential data may be processed (obtained, held, used, disclosed and disposed of). It applies to computerised processing of personal data as well as paper-based files.

5.2 This policy relates to all personal confidential data held by the Trust relating to patients and staff. Personal data is any information, held in any format that relates to a living individual and where that person can be identified from the data contents or from the data contents and other information in the possession of, or likely to come into the possession of, the Trust.

5.3 Staff should only have access to personal confidential data or create records containing personal confidential data in the following circumstances:

- Where the member of staff has a 'legitimate relationship' with the data subject eg: a staff member who is currently providing care to a patient or a member of payroll who is processing an expenses form. This description includes both healthcare professionals and administrators, e.g. ward clerks, medical secretaries, receptionists etc;
- Where the member of staff is the line manager of another employee or is authorised to access personnel files eg: HR staff, department

administrator etc; and

- Where the member of staff is authorised to access personal records / create records in specific circumstances eg:
  - Legal services staff in the case of Subject Access Requests, medico-legal cases, complaints and enquiries;
  - Clinical auditors;
  - Researchers;
  - Health and safety officers;
  - Investigating officers;
  - Finance staff for recharging Commissioners for patients' treatments; and
  - Information services team for managing data quality.

5.4 Our patients and staff expect that information about them will be treated as confidential. Those persons who feel that their confidence has been breached are entitled to lodge a complaint under the NHS Complaints Procedure or lodge a complaint with the Information Commissioner's Office who may take legal action against the Trust.

5.5 A principle aim of the DPA is to promote openness about the processing of personal data and, therefore, the Trust must ensure that any person about whom data is recorded, is aware of the reason their data is collected, its uses within the Trust, to whom it may be disclosed and the circumstances surrounding when it may be disclosed.

5.6 Although the DPA can only be applied to living individuals, a duty of confidence is still owed to the deceased and their families, so this policy includes information on the Access to Medical Records Act 1990 and the common law duty of confidence to provide guidance on this type of data.

5.7 The underlying DPA principle is that all information that can be related to a living individual must be treated as confidential and it must not be communicated to anyone who is not authorised to receive it. Unauthorised persons include staff not involved in either the clinical care of a patient or the associated administration processes. In the case of staff records, unauthorised persons include staff not involved in the management of that member of staff or associated administrative processes.

6 INFORMATION ASSET REGISTER

6.1 Under the DPA, data subjects are entitled to see all information that the Trust records about them in all paper and electronic systems, via a Subject Access Request. To enable this, the Trust must know where the person identifiable data is recorded and stored.

6.2 The ICT Department maintains an Information Asset Register to facilitate this, and to enable the Trust's DPA registration to be kept up-to-date.

7 ACCESS TO KEY COMPUTER SYSTEMS AND HEALTH RECORDS

7.1 There are access control systems in place to ensure that appropriate access is

provided to key computer systems for those members of staff who require access as part of their role. These procedures are detailed in the relevant system procedural documents.

7.2 The Trust operates a 'closed' Medical Records Library (MRL). Only authorised staff are permitted to request health records, and only authorised staff and authorised visitors are permitted to visit the MRL. The MRL supply health records to authorised staff, as detailed in the Health Records Management Policy.

7.3 All health records should be kept as secure as possible, taking into account the constraints of the physical layout of the hospital. As far as possible, there should be a barrier (eg locked filing cabinets, passwords on computer systems, locked office doors etc) between the health records and unauthorised persons.

8 NEW SYSTEMS AND UPGRADES / RELEASES TO EXISTING SYSTEMS

8.1 All new systems and upgrades / releases to existing systems must be assessed prior to implementation to establish whether any person identifiable data will be processed and, if so, to ensure DPA compliance is maintained and to ensure the Trust's registration with the Information Commissioner's Office is kept up-to-date. This is achieved via the 'Information Governance checklist for projects / system releases' (IG Checklist), which is a risk management process. The new system / upgrade / release must be deemed as compliant and approved by the SIRO prior to implementation.

9 RELEVANT LEGISLATION, STATUTORY DUTIES AND GUIDANCE

9.1 The following information is a summary of legislation relevant to the protection and use of person identifiable information. All staff should be aware of their responsibilities under these Acts and have due regard for the law when collecting, using or disclosing confidential information.

9.2 General Data Protection Regulation 2016

9.2.1 The EU General Data Protection Regulation (GDPR) was approved in 2016 and became directly applicable as law in the UK from 25th May 2018. The current Data Protection Act 2018 (DPA18), fills in the gaps in of the GDPR, addressing areas in which flexibility and derogations are permitted.

9.2.2 The GDPR is not directly applicable in the UK post Brexit –but the DPA18 ensures continuity by putting in place the same data protection regime in be UK law pre- and post-Brexit, to create a data protection regime in the UK equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

9.2.3 The headlines are:

- New accountability requirement means organisations are now required, not only to comply with the new law, but to demonstrate that they comply with the new law. In particular, there is a requirement to keep records of data processing activities;

- Significantly increased penalties possible for any breach of the Regulation – not just data breaches;
- Legal requirement for personal data breach notification to the Information Commissioner's Office (ICO) within 72 hours where risk to data subjects;
- Removal of charges, in most cases, for providing copies of records to patients or staff who make a subject access request;
- Requirement to keep records of data processing activities;
- Appointment of a Data Protection Officer mandatory for all public authorities;
- Data protection impact assessments required for high risk processing;
- Data protection issues must be addressed in all information processes at an early stage;
- Specific requirements for transparency and the provision of information to data subjects about how their information is used;
- Provision of healthcare and managing healthcare systems is the main legal basis for the Trust. Consent is another legal basis, and is not always essential if another law requires us to process personal information (example, other health and social care law, employment law, and so on).

Data Protection Act 2018

9.2.1 The Data Protection Act 2018 came into force on 25 May 2018 (the "**Act**"). The Act incorporates the much anticipated EU General Data Protection Regulation (the "**GDPR**") into law in the UK, and supplements its provisions.

9.2.2 The key sections of the Act are:

- **Data Subject Rights**: The Act provides exemptions to the rights individuals have over their personal data under the GDPR. Most of these are a continuation of existing exemptions; for example, personal data will not have to be produced in response to an access request if subject to legal professional privilege or it could reveal information that could prejudice ongoing negotiations. The broadening of the exemption for confidential employment references has already received some comment – it will now be easier to withhold employment references from release. As the scope of rights has broadened considerably, organisations are likely to need to apply more focus to recognising, and responding appropriately to requests received from individuals;
- **Special Category Personal Data**: The Act supplements the GDPR's provisions relating to special category data. For example, when processing data relating to criminal convictions for the purposes of employment, employers are required to maintain an "appropriate policy document". This policy should set out the organisation's procedures for securing compliance with the data protection principles (Article 5 of the GDPR), as well as its retention policies. Provision is also made for specific situations such as processing for the purposes of research, public health, journalism and the prevention of fraud;

- **Data Protection Fee:** The 'notification' regime that existed under the Data Protection Act 1998 has been replaced by an obligation to pay an annual data protection fee. The fee ranges from £40 to £2,900 depending on the size of an organisation. Failure to pay the fee, or paying incorrect fees, can result in a fine of up to £4,350. Organisations currently registered under the previous 'notification" regime may continue to rely on that until their registration comes up for renewal;
- **Consent from children:** In relation to 'information society services' e.g. websites and apps, the Act specifies that a child can provide 'consent' for the purposes of the GDPR from the age of 13 years; this is substantially lower than the default age of 16 years under the GDPR (although Member States were granted the discretion to lower it to 13). Verifiable parental consent will be required for the processing of personal data of children under 13.
- **Data Protection Offences:** New criminal offences have been introduced, including knowingly or recklessly re-identifying information that was previously de-identified (s.171) or deliberately altering or concealing information which should be provided in response to a data subject access request (s.173). It also continues to be an offence to knowingly or recklessly obtain or disclose personal data without the consent of the controller (s.170); and
- **Enforcement:** The Information Commissioner's enforcement powers are set out in the Act. These include enhanced powers to serve information and assessment notices, and to enter and inspect premises in certain circumstances. They are backed up by criminal sanctions (s.148) for destroying or falsifying information to prevent the ICO's staff from accessing relevant information.

9.3 Data Protection (Processing of Sensitive Personal Data) Order 2000

9.3.1 This order sets out additional circumstances where sensitive person identifiable data may be processed. For example, in the prevention or detection of any unlawful act if 'in the substantial public interest'.

9.4 Confidentiality: NHS Code of Practice

9.4.1 This guidance lays down the required practice for those who work for NHS organisations, concerning confidentiality and patients' consent to the use of their health records. The Trust has implemented the requirements through the 'Confidentiality Code of Conduct', which is available via the intranet.

9.5 Computer Misuse Act 1990

9.5.1 The Computer Misuse Act 1990 makes it illegal to access data or computer programs without authorisation.

9.5.2 The Computer Misuse Act establishes three offences. It is illegal to:

- Access data or programs held on computer without authorisation (e.g., to view test results for a patient when you are not directly involved in their care, or to obtain or view information about friends and relatives). On

conviction, an offender is liable to a custodial sentence of six months, a fine of up to £2000 or both;

- Access data or programs held in a computer without authorisation with the intention of committing further offences, e.g. fraud or blackmail. On conviction an offender is liable to a custodial sentence of up to five years, a fine of up to £5000 or both; and
- Modify data or programs held on computer without authorisation. On conviction an offender is liable to a custodial sentence of up to five years, a fine of up to £5000 or both.

9.6 Human Rights Act 1998

9.6.1 Two articles under this Act are relevant to confidentiality of person identifiable data:

- Article 8: Right to respect for private and family life; and
- Article 10: Freedom of expression and exchange of information and opinions.

9.6.2 These articles relate to preventing disclosure of information received in confidence.

9.7 National Health Service Act 2006: Section 251

9.7.1 This section of the Act makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. The Ethics and Confidentiality Committee of the National Information Governance Board for Health and Social Care decides when this temporary measure can be utilised. Please see the Caldicott Guardian for further details.

9.8 Freedom of Information Act 2000

9.8.1 This Act requires Public Authorities (such as the Trust) to routinely provide information about how their organisation works and how decisions are made on services (non-personal data). This Act does not change the right of patients or staff to confidentiality of their person identifiable data.

9.9 Processing of Sensitive Personal Data (Elected Representatives) Order 2002

9.9.1 This order provides Elected Representatives with certain rights over the disclosure of patient's person identifiable data. The Trust has decided that all requests for information will be dealt with via the Complaints and Legal Services Department to ensure appropriate disclosure of person identifiable data, in accordance with the Data Protection Act 1998 and this order.

9.10 Common Law Duty of Confidence

9.10.1 The basic principle in relation to the common law duty of confidence is that patient information is confidential to the patient and should not generally be disclosed without consent, unless justified for a lawful purpose (required by

statute).

9.10.2 This principle is now replicated in legislation, however, the common law duty still applies and in some circumstances requires consideration in addition to the legislation e.g. where explicit patient consent is required before it can be used for non-healthcare purposes.

9.10.3 Every member of staff is responsible for ensuring that:

- Patient and staff information is only used for specified and lawful purposes and that confidentiality is respected; and
- They understand and comply with the law and if in doubt, seek advice from the IG Committee members. Contact details are on the IG intranet site.

9.11 Access to Health Records Act 1990

9.11.1 This Act entitles individuals, subject to certain exemptions, to access health information held about deceased persons. The patient's family often appoints a solicitor to deal with these requests. All access to Health Records Act requests are dealt with by the Complaints & Legal Services Department.

9.12 Legal Restrictions on Disclosure

9.12.1 Sexually Transmitted Diseases

All necessary steps must be taken to ensure that any data capable of identifying an individual with respect to examination or treatment for any sexually transmitted disease (including HIV and AIDS) shall not be disclosed except:

- Where there is explicit patient consent to do so;
- For the purpose of such treatment or prevention; and
- For the purpose of communicating that data to only those staff directly involved with the treatment of persons suffering from such disease or the prevention of the spread thereof.

9.12.2 Human Fertilisation & Embryology Act 1990

Disclosure restrictions apply to treatments where individuals can be identified. Generally explicit consent is required, except in connection with the:

- Provision of treatment services, or any other description of medical, surgical or obstetric services, for the individual giving the consent; and
- Carrying out of an audit of clinical practice.

9.12.3 Abortions Regulations 1991

These regulations limit and define the circumstances in which information may be disclosed.

9.13 **Caldicott Principles**

9.13.1 Following the Caldicott Committee's Report on the Review of Patient Identifiable Information published in December 1997, every NHS Trust has a duty to appoint a Caldicott Guardian. The Trust's Caldicott Guardian is Alistair Steel - Consultant Anaesthetist.

9.13.1 The Caldicott principles are concerned with the use and protection of patient identifiable information. All Trusts must abide by the principles for all patient identifiable information flows:

- **Principle 1** - Justify the purpose(s) for using confidential information
- **Principle 2** - Only use it when absolutely necessary
- **Principle 3** - Use the minimum required
- **Principle 4** - Access should be on a strict need-to-know basis
- **Principle 5** - Everyone must understand his or her responsibilities
- **Principle 6** - Understand and comply with the law

A second Information Governance Review was undertaken in 2012/2013 and the report, issued in March 2013, included a 7th principle:

- **Principle 7** - The duty to share information can be as important as the duty to protect patient confidentiality.

10 REFERENCES

10.1 **References to Standards**

- Information Governance Toolkit v.15

10.2 **Legislation**

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Computer Misuse Act 1990
- Data Protection Act 2018
- European Union General Data Protection Regulation 2016
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Freedom of Information Act 2000
- Human Rights Act 1998
- National Health Service Act 2006
- Processing of Sensitive Personal Data (Elected Representatives) Order 2002

10.3 **Guidance**

- Report on the Review of Patient Identifiable Information (Caldicott Report) 1997
- The Information Governance Review (Caldicott2 Report) March 2013
- The Caldicott Guardian Manual 2010
- Records Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- Information Security Management: NHS Code of Practice
- ISO/IEC 27001: 2005 Information Security Management Standards
- Information Commissioners Guidance – Use and Disclosure of Health

11 ARRANGEMENTS FOR MONITORING COMPLIANCE WITH THIS POLICY

11.1 Compliance with this policy will be monitored in the following manner (see table below):

Key elements (Minimum Requirements)	Process for Monitoring (e.g. audit)	By Whom (Individual / group /committee)	Frequency of monitoring
Reducing the number of confidentiality breaches	Management of incidents relating to Data Protection	IG Team	Monthly
Roles and responsibilities	Monitored at appraisal, following review of the individual's knowledge & skills framework (KSF) together with the job description.	Line manager	Annually
How the organisation provides Data Protection Training. In house training sessions are delivered regularly throughout the year to meet the needs of the Trust	Electronic Staff Record (ESR) is utilised to identify all staff who are non-compliant	IG Team	Monthly
Ensuring best practice across the Trust	Undertaking Confidentiality Audits	IG Team	Monthly

APPENDIX 1

EQUALITY IMPACT ASSESSMENT
Equality Impact Assessment Tool
(To be completed and attached to any policy document when submitted to the appropriate committee for ratification.)
STAGE 1 - SCREENING

Name & Job Title of Assessor: Phil Cottis – IG & RA Manager	**Date of Initial Screening: 27/09/11**
Policy or Function to be assessed: Data Protection Policy	

		Yes/No	Comments
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**		
	• Race & Ethnic background	No	
	• Gender including transgender	No	
	• Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	

Signature of Assessor: Phil Cottis **Date: 13th September 2018**
Head of Health Records

Signature of Line Manager: Jon Wade **Date: 13th September 2018**
Chief Operating Officer