Our Vision
The best care for every patient

NHS
Norfolk and Norwich University Hospitals
NHS Foundation Trust

Data Protection and Confidentiality Policy

For Use in:	Organisation-wide
By:	All Staff Groups
For:	All Staff
Division responsible for document:	Corporate
Key words:	Data Protection, Data Protection Principles, Caldicott principles, Privacy Impact Assessment, Confidentiality Audit, Monitoring, Right of Access, Registration, Personal information, Confidentiality Audit, safeguarding
Name of document author:	Vimmi Lutchmeah-Beeharry
Job title of document author:	Head of Information Governance
Name of document author's Line Manager:	Ben Everitt
Job title of author's Line Manager:	Associate Director – Digital Health
Supported by:	
Assessed and approved by the:	**Caldicott and Information Governance Assurance Committee** **If approved by committee or Governance Lead Chair's Action; tick here ☐**
Date of approval:	30/08/2022
Ratified by or reported as approved to (if applicable)**:**	**Digital Health Committee**
To be reviewed before: This document remains current after this date but will be under review	29/08/2025
To be reviewed by:	Head of Information Governance
Reference and / or Trust Docs ID No:	**718**
Version No:	**7.3**
Compliance links: *(is there any NICE*	Data Security and Protection Toolkit

related to guidance)	
If Yes - does the strategy/policy deviate from the recommendations of NICE? If so why?	

Version and Document Control:

Version No.	Date of Update	Change Description	Author
7	November 2020	Full review in line with data opt out	VLB
7.1	March 2021	• Added the 8th Caldicott principles context and principles • Updated the Caldicott Guardian details • Replaced Data Protection Bill by data Protection Act 2018 • Replaced Data Retention & Erasure Policy by Data Retention & Disposal Policy • Minor typos	VLB
7.2	December 2021	• Minor edit, NHSx replaced DoH • ICO financial penalty amount	VLB
7.3	August 2022	• Added the reference to Article 4 of the UK GDPR the third para of the scope to cover all personal data • Expanded the scope to specifically mention images following a recommendation made by an external body for an IG SIRI	VLB

This is a Controlled Document

Printed copies of this document may not be up to date. Please check the hospital intranet for the latest version and destroy all previous versions.

Contents page

1. Introduction

Norfolk and Norwich University Hospitals NHS Foundation Trust (hereinafter referred to as the **"The Trust"**) needs to collect personal information to effectively carry out everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes (but is not limited to), name, address, email address, date of birth, IP address, identification numbers, private and confidential information, sensitive information and bank details.

In addition, The Trust may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however the Trust are committed to processing all personal information in accordance with the **UK General Data Protection Regulation (GDPR)**, **UK Data Protection Law** and any other relevant Data Protection Law and codes of conduct (herein collectively referred to as **"Data Protection Legislation"**).

The Trust has developed policies, procedures, controls and measures to ensure the proportionate satisfaction of Data Protection Law and its principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and the Trust are proud to operate a **'Data Protection by Design'** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

The Trust has a legal obligation to comply with the Data Protection Law, the Confidentiality Code of Conduct, the Caldicott principles and related guidance set by the Department of Health to provide assurance to its staff, patients and any contracted third parties that:

Personal Confidential Data (PCD) are handled properly

There is enough protection to safeguard the data

There is adequate control when there is a need a share this information with any third parties.

a. Caldicott Principles

The late National Data Guardian for Health and Social Care (NDG) Dame Fiona Caldicott has published the outcomes from a public consultation that she ran to seek views on her intention to:

- revise the existing 7 Caldicott Principles
- introduce a new principle about ensuring there are no surprises for patients and service users about the use of their confidential information
- issue guidance about the role of Caldicott Guardians using her statutory powers

The consultation response contains a revised – and expanded – set of 8 Caldicott Principles and includes a commitment to issue guidance about Caldicott Guardians in 2021.

The Caldicott Principles, first introduced in 1997 and previously amended in 2013, are guidelines applied widely across the field of health and social care information governance to ensure that people's data is kept safe and used appropriately. Caldicott Guardians support the upholding of these principles at an organisational level.

The new principle's purpose is to make clear that patient and service user expectations must be considered and informed when confidential information is used, to ensure 'no surprises' about the handling or sharing of their data.

A detailed explanation of the ***Eight*** Principles can be found at Appendix 1.

b. The Health and Social Care Guide to Confidentiality 2013

The HSCIC Guide to Confidentiality 2013 shows health and care workers what they should do and why, to share information safely while following rules on confidentiality. It covers the five confidentiality rules:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

c. Common Law Duty of Confidentiality

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. This is a legal obligation that is derived from case law, built up over many years.

This Common Law Duty of Confidentiality places an obligation on all individuals working in and for the Trust to ensure all confidential information which they come into contact with is kept secure and confidential at all times even when they cease to work for the Trust.

Whilst the Data Protection Law only covers living individuals' information, the Common Law Duty of Confidentiality ensures a patient's right to Confidentiality continues after their death.

d. General Data protection Regulation (GDPR) principles

The purpose of the Regulation is to protect the rights and privacy of individuals, and to ensure data about them is not processed without their knowledge or consent wherever possible.

The Act covers personal data relating to living individuals.

The Act stipulates that any organisation processing personal data must comply with the following **six Data Protection Principles**.

Lawfulness, fairness & transparency' - processed lawfully, fairly and in a transparent manner

Purpose limitation - collected for specified, explicit & legitimate purposes

Data minimisation - adequate, relevant & limited to what is necessary

Accuracy - accurate and kept up to date

Storage limitation' - kept for no longer than is necessary

Integrity & confidentiality' - ensures appropriate security

The accountability principle requires The Trust to take responsibility for what you do with personal data and how you comply with the other 6 principles given above.

An explanation of the Six Data Protection Principles can be found at Appendix 2.

2. Purpose

This Data Protection and Confidentiality Policy defines the legal framework that governs the confidentiality of all information held by the Trust by detailing its legal obligations under the General data protection Regulation and The UK Data Protection Law which underpins the NHS Confidentiality Code of Practice, 2003 that all staff must comply with and the Health and Social Care Confidentiality Practice

The Trust is continually changing its processes and systems to further improve the Trust's proportionate satisfaction with Data Protection Law and staff are responsible for ensuring they keep up to date with Trust policies, procedures and guidance.

Whilst working for the Trust, staff will have access to information about patients and/or about the Trust. Staff may find this information out as part of their work, see, hear or read something while on Trust premises. This information should be kept confidential even after their contract ends with the Trust.

All staff have a legal obligation to ensure any confidential information they come into contact with is kept secure and confidential at all times. If there is a need to disclose any personal identifiable information, staff must ensure that any disclosure of such

information is fully justified and satisfies the GDPR, UK Data Protection Law, Caldicott principles and the Common Law Duty of Confidentiality.

Where staff are unsure of whether to disclose the requested information or not, they MUST seek advice from their immediate Supervisor/Manager or if this is not possible seek advice from or direct the person making the request to the Trust's Head of Information Governance - Data Protection Officer, Legal Department and/or Caldicott Guardian.

3. Scope

The **Health and Social Care Guide to Confidentiality 2013** outlines the working practices an NHS Trust must adopt in order to deliver patient confidentiality required by law, ethics and policy, with an objective of continuous improvement.

All legislations relevant to an individual's right of confidence and the ways in which these are handled are very important to the Trust. This relates to all information held in the Trust relating to all its patients, staff and any other individual who comes into contact with the Trust.

The Data Protection principles applies to all records containing personal data as defined in Article 4 of the UK GDPR, both in electronic and paper formats that identifies, or any records that could identify an individual whose records are held and processed by the Trust.

This Data Protection principles covers the use of images of individuals, including photos and videos, for the Trust's own purposes. It applies to images already stored on the Trust's databases and shared folders, as well as to images captured in the future.

The Trust as a "Data Controller" is responsible for all records detailed above and is registered with the Information Commissioner's Office (ICO) bearing Registration No. Z5023551**.** The Trust notification of processing is accessible by any member of the public through the ICO's website and no advice is given as what is going to be displayed post 25th May 2018 when GDPR was enforced.

Post 25th May 2018, The Trust has a legal duty to keep a Data Processing Activities Log detailing all the data processing the Trust carries out. This log should be disclosed upon request to the Supervisory Authority when required.

The policy will apply to:

All information used by the Trust;

All information systems managed by or for the Trust;

Any individual using information 'owned' by the Trust;

Any individual requiring access to information 'owned' by the Trust;

Any individual working on behalf of the Trust, or anyone who accesses Trust premises

and information which is owned or managed by the Trust.

4. Objective

The Trust is committed to ensuring that all personal data processed by the Trust is done so in accordance with the proportionate satisfaction of Data Protection Law and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. The Trust shall ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Trust has considered and agreed the below policy principles to meet our data protection obligations and to ensure the continuous proportionate satisfaction of legal and regulatory requirements.

The Trust ensures that:

The Trust shall consider lawfulness, fairness and proportionality as the overriding outcome to expect from how it exercises and applies its data protection and confidentiality authority and obligations

The Trust shall protect the rights of individuals with regards to the processing of personal information.

The Trust shall develop, implement and maintain a risk based data protection policy, procedure, audit plan and training program for satisfying data protection law.

Every business practice, function and process carried out by the Trust, is monitored for the proportionate satisfaction with the Data Protection Law and its principles.

Personal data shall only be processed where we have verified and met the lawfulness of processing requirements.

The Trust shall process special category data in accordance with the GDPR requirements and in satisfaction with the Data Protection Act 2018 - Schedule 1 conditions.

The Trust shall process criminal conviction data in accordance with Part 2, of Schedule 2 of the DPA 2018

All employees are competent and knowledgeable about their GDPR obligations and are provided proportionate training in the data protection law, principles, regulations and how they apply to their specific role and the Trust.

Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection law.

The Trust shall maintain a continuous risk based program of monitoring, review and improvement with regards to the proportionate satisfaction with the Data Protection Law.

The Trust shall monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements.

The Trust shall have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.

The Trust shall appoint ***a Data Protection Officer*** who will take responsibility for the overall supervision, implementation and ongoing assurance with the Data Protection Law and performs specific duties as set out under Article 37 of the GDPR.

The Trust have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued assurance. This also forms part of the Data Security and Protection Toolkit audit conducted by the Trust Internal Auditors on an annual basis.

The Trust shall provide clear reporting lines and supervision with regards to data protection.

The Trust shall store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes.

Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Employees are aware of their own rights under the Data Protection Law and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice.

Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements.

The Trust shall develop and implement appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place.

5. Glossary

The following terms and abbreviations have been used within this document:

Term	Definition
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Binding Corporate Rules	Personal data protection policies which are adhered to by the Trust for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
Consent	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear

	affirmative action, signifies agreement to the processing of personal data relating to him or her.
Cross Border Processing	Processing of personal data which: takes place in more than one Member State; or which substantially affects or is likely to affect data subjects in more than one Member State
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data protection law	For the purposes of this document, the collective description of the GDPR, Data Protection Act 2018 and any other relevant Data Protection Law that the Trust complies with.
Data subject	An individual who is the subject of personal data
GDPR	General Data Protection Regulation (EU) (2016/679)
Fairness	In general, fairness means that processing must be done in ways that people would reasonably expect and not in ways that have unjustified adverse effects on them. Assessing whether processing is fair depends in part on how the data was obtained and how the processing affects individuals.
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Proportionate / Proportionality	This requires that the action of the organisation be appropriate for attaining the legitimate objectives pursued by the organisation and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives i.e. the extent to which there is a logical link between the measure and the (legitimate) objective pursued, and the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of privacy rights and issues.
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Supervisory Authority	An independent public authority which is established by a Member State.
Third Party	A natural or legal person, public authority, agency or body other than the data controller, data processor data subject, or persons under the direct authority of the Trust as a data controller.

6. Duties

a. Chief Executive Officer

The Chief Executive Officer has overall responsibility for the Data Protection Policy within the Trust. The implementation of, and proportionate satisfaction with this Policy is delegated to the Senior Information Risk Owner, Caldicott Guardian and designated Data Protection Officer, the members of the Information Governance Steering Group and the Caldicott Advisory Group.

b. The Senior Information Risk Owner (SIRO)

The SIRO is responsible for ownership of the Trust's Information Risks, to act as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of their Statement of Internal Control in relation to information risk. The Trust's SIRO is the Chief Information Officer.

c. Caldicott Guardian

The Caldicott Guardian is responsible for advising on the uses of patient information within the Trust and acting as the 'conscience' of the Trust in matters relating to patient confidentiality.

The Caldicott Guardian advises on options for lawful and ethical processing of information as required. The Trust's Caldicott Guardian is the Chief Clinical Information Officer.

d. Data Protection Officer

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on organisations to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by the organisation where:

- The processing is carried out by a public authority or body (except for courts acting in their judicial capacity).
- The core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.
- The core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
- The Trust designated Data Protection Officer (DPO) is the Head of Information Governance and in accordance with GDPR requirements have ensured the designated person has an adequate and expert knowledge of data protection law.

See Appendix 6 for Data Protection Officer's Tasks.

e. The Head of Information Governance – Data Protection Officer

The Head of Information Governance is the Trust designated Data Protection Officer and performs the following:

Maintaining Data Processing Activities Log and the Register of processing activities (ROPA);

Developing and delivering training;

Develop policies, procedures and guidance for staff to support their understanding and compliance with this policy;

Managing the Trust's Data Protection and Subject Access Requests;

Acting as main point of contact for any data protection issues which may arise within the Trust;

Support the Trust's Caldicott Guardian and the SIRO;

Management of incidents and Complaints relating to personal data which occur at the the Trust.

f. The Information Security Manager

The Information Security Manager will support the Data Protection Officer in the above tasks and will act on their behalf during their absence.

g. Managers / Heads of Department / Information Asset Owners

Data Protection procedures will vary from department to department and across disciplines. It is the responsibility of Managers/Heads of Department to ensure adequate and compliant procedures are developed to handle personal data and sensitive personal data.

Managers and Heads of Department may delegate the day to day running of operational procedures but may not delegate overall responsibility for the handling of personal data and sensitive personal data within their departments. They are also responsible for promoting the reporting of Data protection and Confidentiality breaches on the Trust Incident Reporting System – DATIX.

It is the responsibility of the Trust's delegated Information Assets Owners to ensure all information assets are documented and kept appropriately secure, in line with the Data Protection Principles and are not kept for longer than necessary.

The Information Asset Owners will support the Head of Information Governance with the Data Protection Impact Assessment process.

Information Asset Owners will be supported by Information Asset Administrators, but the overall responsibility for the management of the Trust information assets sit with the Information Asset Owners.

h. Information Asset Administrator

Each computer system/database will have a designated information asset administrator. A list of these nominated personnel will be maintained as part of the Asset inventory which forms part of the Trust's Information Security Management System.

All Information Asset Administrators will ensure that all systems/databases which require registration are registered in accordance with the Data Protection Law requirements and these registrations are reviewed on a regular basis.

All Information Asset Administrators will sign a System Administrator Elevated Privileges Agreement.

i. All Staff

All employees of the Trust who process personal data in any form must ensure they comply with the requirements of the Data Protection Law and the Trust's Data Protection and Confidentiality Policy, including any procedures and guidelines which may be issued through Communication or published on the Trust Intranet site.

All staff are responsible for ensuring they complete their mandated Information Governance Training and to understand the key principles of the Data Protection Act, how this applies to Trust policies, procedures and guidance.

All queries about this Policy should be directed to the Information Governance Team.

All staff are responsible for reporting Data protection and Confidentiality breaches as well as any other incidents on the Trust Incident Reporting System – DATIX.

All staff are made aware it is an offence under the Data Protection Act for viewing their own records and those of families, friends and colleagues. As a consequence this may be considered as a gross misconduct which may result in immediate dismissal or suspension until a complete investigation is carried out. A non-exhaustive list of offence includes:

- Unlawful disclosure of Personal Data and/or Sensitive Personal Data.
- Inappropriate use of Personal Data and/or Sensitive Personal Data.
- Misuse of the Personal Data and/or Sensitive Personal Data which results in any claim being made against the Trust.
- Loss of Personal Data and/or Sensitive Personal Data.
- Unauthorised disclosure or copying of information belonging to the Trust
- Unauthorised access to any clinical systems
- Abuse of granted privileges, such as looking at your own/your relatives/your friends/colleagues clinical records on the clinical system or the Summary Care record or the Electronic Staff Record (ESR). In such circumstance, access to the respective system will be revoked until investigation is completed.

7. Processes to be followed

a. Notification to the Information Commissioner

The Trust has a legal obligation as a Data Controller to register with the commissioner, The Supervisory Authority, who will oversee the satisfaction of Data Protection requirements.

The Trust will review on an annual basis the purposes for which its processes information to ensure that the Trust's processing of data and updates the Data Processing Activities Log.

Individual data subjects can obtain details of the Trust's Data Protection registration from the Information Commissioner's Office (ICO) website. At the time of writing this policy the future of the Register of Data Controllers' on the ICO website is unknown.

b. Processing

The Trust uses the HORUS - Holding, Obtaining, Recording, Using and Sharing acronym to define '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:

Organisation, adaptation, alteration of the information or data;

Retrieval, consultation or use of the information or data;

Disclosure of the information or data by transmission, dissemination or otherwise making available; or

Blocking, deletion/erasure or destruction of the information or data.

c. Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by the Trust, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection law and can evidence such measures through our documentation and practices.

Our main accountability intentions are to:

Educate senior management and employees about the requirements under the data protection law and the possible impact of non-satisfaction of the Trust requirements

Provide a dedicated and effective data protection training program for all employees

Identify key stakeholders to support the data protection framework program

Allocate responsibility for data protection and ensure the designated person(s) has sufficient access, support and budget to perform the role

Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures the Trust has in place to ensure and demonstrate assurance with data protection law, regulations and codes of conduct, are detailed in this document and associated information security policies.

d. Privacy by Design

The Trust will operate a 'Data Protection by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. The Trust have developed controls and measures (detailed below), that help us enforce this ethos.

7.d.1 Approach

The Trust shall apply a risk based Information Governance approach to implementing and satisfying its data protection and confidentiality plans and obligations

7.d.2 Data Minimisation

Under Article 5 of the GDPR, principle (c) advises data should be 'limited to what is necessary', which forms the basis of our minimalist approach. The Trust only obtain, retain, process and share data essential for carrying out tasks and/or meeting legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our assurance with the data protection law.

Measures to ensure only the necessary data is collected includes:

Electronic collection (i.e. forms, website, surveys, etc.) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain.

Physical collection (i.e. face-to-face, telephone, etc.) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only which is relevant and necessary is collected.

The Trust have SLA's and bespoke agreements in place with third-party controllers who send us personal information (either in our capacity as a controller or processor). These state only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.

The Trust shall have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.

Forms, contact pages and any documents used to manually collect personal information are reviewed every 3-months to ensure they are fit for purpose and only collecting necessary personal information in relation to the legal basis being relied upon and for the purpose of processing. If the purpose has been served these should be transferred to the relevant documentation such as the patient or staff folder before being permanently destroyed in a confidential manner.

7.d.3 Pseudonymisation

The Trust utilise pseudonymisation where possible to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (personal identifiers). Encryption and partitioning is also used to protect the personal identifiers, being kept separate from the pseudonymised data sets.

When using pseudonymisation, the Trust ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

7.d.4 Restriction

Our Privacy by Design approach means we use Trust-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Trust's processes, systems and structure and ensures only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by staff who need them to perform their role.

7.d.5 Hard Copy Data

Due to the nature of our business and as we do not have an electronic patient record system, it is essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (i.e. copies of patient records, hospital invoices or claims information). We aim to keep these records secure at all times.

e. Information Audit

To enable the Trust to fully prepare for and comply with the data protection law, we have carried out a Trust-wide data protection information audit to better enable us to record, categorise and protect the personal data we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our Trust in our capacity as a controller/processor and has been compiled on a central register which includes: -

What personal data we hold

Where it came from

Who we share it with

Legal basis for processing it

What format(s) is it in

Who is responsible for it?

Disclosures and Transfers

f. Legal Basis for Processing (Lawfulness)

At the core of all personal information processing activities undertaken by the Trust, is the assurance and verification we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations.

Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where:

The data subject has given consent to the processing of their personal data for one or more specific purposes

Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

Processing is necessary for compliance with a legal obligation to which we are subject

Processing is necessary in order to protect the vital interests of the data subject or of another natural person

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust

Processing is necessary for the purposes of the legitimate interests pursued by the Trust or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

g. Processing Special Category Data

Special categories of Personal Data are defined in the Data Protection Law as:

'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies'.

The Trust processes personal information classed as special category – Health data or information relating to criminal convictions, we do so in accordance with Article 9 of the

GDPR regulations and in line with the Data Protection Act 2018 Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We process special category data where:

The data subject has given explicit consent to the processing of the personal

Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

Processing is necessary for reasons of public interest in the area of public health

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Schedule 1, Parts 1, 2 & 3 of The Data Protection Act 2018 provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

h. Safeguarding

Staff must continue to share information to the Local Authority, MASH and other agencies when a safeguarding concern is raised and nothing within the GDPR affects that duty. For the purpose of safeguarding children and vulnerable adults, the Trust can rely upon Articles 6 and 9 when processing and disclosing information relating to a safeguarding query without a patient's consent namely.

i. Records of Processing Activities

As an organisation with 250 or more employees the Trust maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.

Acting in the capacity as a controller our internal records of the processing activities carried out under our responsibility, contain the following information: -

Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, we also record any joint controller and/or the controller's representative

The purposes of the processing

A description of the categories of data subjects and of the categories of personal data

The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organisations)

Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)

Where possible, the envisaged time limits for erasure of the different categories of data

A general description of the processing security measures as outlined in section 12 of this document (pursuant to Article 32(1) of the data protection law)

As part of our obligations under the UK's Data Protection Act 2018, Sch.1, Pt.4, where we are required to maintain a record of our processing activities in our capacity as a controller and are processing special category or criminal conviction data, as specified in Sch.1, Pt.1-3 of the Act 2018, we also record the below information on the register:

Which condition is relied on?

How the processing satisfies Article 6 of the Data Protection Law(*lawfulness of processing*)

Whether the personal data is retained and erased in accordance with the policies described in paragraph 30(b) of the DP Act 2018 (*and if not, the reasons for not following those policies*).

8. Data Protection Rights Procedure

a. Information Provision

Where personal data is obtained directly from the individual (i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc.), we provide the below information in all instances, in the form of a privacy notice:

The identity and the contact details of the controller and, where applicable, of the controller's representative

The contact details of our data protection officer

The purpose(s) of the processing for which the personal information is intended

The legal basis for the processing

Where the processing is based on point (f) of Article 6(1) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party", details of the legitimate interests

The recipients or categories of recipients of the personal data (if applicable)

The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability. Please note Health Data is exempted for Erasure.

Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal

The right to lodge a complaint with the Supervisory Authority

Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent unless there is a legal requirement to keep the information longer.

b. Privacy Notice

The Trust defines a Privacy Notice as a document that is provided to individuals or the individuals is directed to the Trust public website at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly).

Our Privacy Notice includes the Article 13 (where collected directly from individual) or 14 (where not collected directly) requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the public facing policy that provides the legal information on how we handle process and disclose personal information. The Privacy notice can be accessed at http://www.nnuh.nhs.uk/departments/information-governance/data-protection/privacy-notice/

c. Employee Personal Data

As per the Data Protection Law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the Data Protection Law and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

Please refer to Appendix 5 for more detail.

d. Right to access personal information (Subject Access Request)

We have ensured appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34.

Such information is provided free of charge in most cases and charges may only apply for admin purposes but this may prove difficult to justify. The process will ONLY start by the relevant Team after the data subject's identity has been verified and the purpose of the request clarified and agreed with the data subject. In the circumstances where disclosure has been asked from third parties, the relevant team should ensure that the data subject has consented for such disclosures.

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is clarified and agreed by the relevant team. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Information Commissioner's Office.

e. Data Portability

The Trust provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read, where possible.

To ensure we comply with Article 20 of the Data Protection Law concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on:

Consent pursuant to point (a) of Article 6(1)

Consent pursuant to point (a) of Article 9(2)

A contract pursuant to point (b) of Article 6(1); and

the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the Trust to a designated controller, where technically feasible.

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

f. Rectification and Erasure

8.f.1 Correcting Inaccurate or Incomplete Data

Article 16 of the GDPR gives individuals the right to request rectification of any inaccurate data held by the Trust or for incomplete data to be completed.

The request can be made verbally or in writing to the Data Protection Officer and the Trust has one calendar month to respond to a request. The Trust can refuse a request for rectification and a record should only be corrected after proper review and reflection by the clinical team.

The ICO has provided guidance on what should be removed or delated from a patient's medical records and great care should be taken before removing. It is important to correct the mistake, this can be done by filing an amended note alongside the original record, furthermore, the original record may have been relied upon and inform a patient's diagnosis and treatment therefore removing that will lead to gaps in the patient's medical history. Also care should be taken to distinguish opinion from facts; Opinions are subjective and should not be corrected. The ICO provides the following helpful example which may help to inform the decision whether to remove an entry or not:

"If a patient is diagnosed by a doctor as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified."

8.f.2 The Right to Erasure

The right to erasure more commonly known as "the right to be forgotten" does not apply to health records and medical records should only be destroyed in accordance with the applicable department of health guidelines which are referred to in the Data Retention and Disposal policy. The patient must be advised of this if they request a record to be erased.

All data will be deleted in line with the Data Retention & Disposal Policy and complying with the Article 17 requirements.

g. Data Protection Impact Assessment

Please refer to the Data Protection Impact Assessment Policy and Procedure (Trust Docs ID: 18157).

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Trust. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the Trust must or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) (sometimes referred to as a Privacy Impact Assessment).

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

Transfer

Reduced

Accepted

Please refer to the Data Protection Impact Assessment policy.

9. Protect personal information

In order to provide a confidential service, The Trust needs to ensure it protects patient information at all times, so only staff that have a business need to access the confidential information can do so.

Staff should check any callers, by telephone or in person, are correctly identified (please refer Appendix 4). There could be a significant risk of harm to a patient through the impersonation by those seeking information improperly

Staff should share the minimum information necessary to provide safe care or to satisfy other legitimate purposes, bearing in mind that missing information can harm patient care.

A patient's confidentiality must be respected in response to enquiries from external individuals or organisations (e.g. media, police, and insurance companies). In these circumstances express consent must be obtained from the patient and/or proper (legal) authority demonstrated before any disclosure is made.

There are some statute disclosures of personal identifiable information which would not require the individual's consent. Some of them are listed below:-

Births and deaths

Notifiable communicable diseases

Poisonings and serious accidents at the work place

Terminations

The misuse of drugs

Offenders thought to be mentally disordered

Child abuse

Domestic Violence

Road traffic accidents

Prevention/detection of a serious crime i.e. terrorism, murder

Staff must not use any of the Trust's IT systems to make an unauthorised disclosures or copy of confidential information belonging to the Trust. Access to any critical patient administration systems are monitored on a monthly basis.

10. Information sharing

Please refer to the Information Sharing Policy (Trust Docs ID: 8306)

The Trust will ensure measures are put in place to INFORM patients what information about them is collected, stored and, if necessary, shared with other professionals and organisations involved with their care and the reasons for this.

Patient clinical information can only be released to someone who has the Lasting Power of Attorney or to someone who the patient has specifically consented or not consented to share his/her clinical information with and the consent should be documented in the medical records.

In circumstances where the patient has a full-time career who is neither the individual holding the power of attorney or an individual the patient has consented to receive such information then staff should ask the patient for consent and/or in cases where the patient cannot give consent staff should contact the individual with the lasting power of attorney to seek their permission.

Where information is being shared with third party providers, contracts must be put in place to address all necessary data protection and information security issues and ensure this complies with the Caldicott principles

The Trust will effectively manage and record, the use and transfer of personal data across all healthcare partners by implementing agreed information sharing protocols or agreements

Each Information Sharing Agreement/Protocol **MUST** be authorised by the Caldicott Guardian or the IG Lead prior to data being shared.

There may be circumstances where there is a need to disclose personal information and none of the above applies. In those cases, it is **VERY IMPORTANT** staff make an assessment of the need to disclose the information and to document all steps taken in reaching that decision, including the requestor details. Further guidance can be obtained from the Head of Information Governance and the Confidentiality Code of Conduct.

All external employees must complete the relevant IG training and signs the confidentiality agreement prior to start of work with the Trust

Where external organisation will have access to The Trust network remotely, they need to comply with the Remote Access Policy.

11. Reporting, Investigating and consequences of loss of personal information

Please refer to the Policy for Managing Information Governance, Information / Cyber Security Related Incidents (Trust Docs ID: 10008)

Any breaches/losses of personal data must be reported using the Trust's Incident reporting process and will be reviewed by the Caldicott Approval Group.

The losses of personal data will be reported in line with the Data Security Protection Toolkit's (DSPT) Incident Reporting tool

The Trust will report all data losses in its annual report as per DSPT guidance.

Breaches of this Policy will be considered a serious disciplinary matter and will be dealt with accordingly. Refer to section 6.10.4.

Consequences of a data breach is a criminal offence under the Data Protection Act 2018 and may include:

Immediate Dismissal

Suspension of access to clinical systems and/or Trust network and premises

Suspension until investigation is completed

Being investigated by the Information Commissioner's Office

Being served a sentence

Individuals may be fined by the Court and/or the Information Commissioner Office

Organisation can be fined by the Information Commissioner's Office.

12. Data Processing Activities

Staff must inform the Information Governance Department, info.gov@nnuh.nhs.uk for any new processing, containing personal identifiable data leaving the Trust.

13. Contracts of employment

Staff contracts of employment are produced and monitored by the Trust's Human Resources department. All contracts of employment include an information governance/data protection and confidentiality clause. Agency and contract staff are subject to the same rules.

The Trust has a Confidentiality agreement non-Trust staff must sign before undertaking any work in or on behalf of the Trust

14. Confidentiality Audit

The Trust will carry regular audit on key Digital Health systems which involves Patient Identifiable Data. The Audit will look at:

Failed attempts to access confidential information;

Repeated attempts to access confidential information;

Successful access of confidential information by unauthorised persons;

Evidence of shared login sessions/passwords;

Investigation and management of confidentiality events will be in line with the Incident Management and Investigation Policy (Trust Docs ID: 15736)

Disciplinary procedures should outline the penalties for unauthorised access or attempts. E.g. suspension, supervised access to systems, ending a contract, employee dismissal or the bringing of criminal charges.

15. Data Opt-Out

Please refer to the Data Opt-Out policy, (Trust Docs ID: 18158)

The data opt-out implements the opt-out model proposed by the National Data Guardian (NDG), as accepted by the Government and directed by the Department of Health and Social Care.

The National Data Guardian's Review of Data Security, Consent and Opt-Outs (NDG Review) proposed that:
"There should be a new consent/opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care".

The NDG's review carefully considered the scope of the model including its limitation to purposes beyond individual care only and for it to be an opt-out rather than consent model:
"3.2.2: The Review was persuaded that the best balance between meeting these expectations and providing a choice to those who have concerns is achieved by providing an opt-out model. The review concluded that people should be made aware of

the use of their data and the benefits; an opt-out model allows data to be used whilst allowing those who have concerns to opt out".

The review also acknowledged that *"Whilst patients have a right under the NHS Constitution to request that their personal confidential data is not used beyond their direct care, there is currently no easy way for them to do that"2.* The national data opt-out provides a single central mechanism which gives effect to this right.

16. Development and Consultation Process

This policy has been circulated to Caldicott and Information Governance Assurance Committee for comments and approval.

This version has been endorsed by the Caldicott and Information Governance Assurance Committee and will be ratified by the Digital Transformation Board.

17. Audit / Monitoring

The Trust will monitor staff compliance against this policy through:-

Reported Trust incidents relating to breaches of confidentiality, loss of personal information.

Regular confidentiality Audit of the critical systems

Departmental satisfaction with this policy will be subject to ad hoc spot checks to assess whether departments are complying and applying the Data Protection Policy.

18. Supporting References

Common Law Duty of Confidentiality

General Data Protection Regulation 2016

Data Protection Act 2018

Children Act 1989

Access to Health Records 1990

Access to Medical Reports Act 1988

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

Computer Misuse Act 1990

Information Commissioner's Office. Available at: http://www.ico.org.uk

Guide to Confidentiality in Health and Social Care(2018)

Care Quality Commission's Review Safe Data, Safe Care (2017)

National Data Guardian's Review of Data Security, Consent and Opt-Outs (2016)

Information Governance: To share or not to share The Information Governance Review

Report (2013)

NHS Confidentiality Code of Practice 2003

NHS Digital Data Security and Protection Toolkit

NHS Digital website

19. Associated Documentation

Information Governance Policy (Trust Docs ID: 725)

Information Governance Strategy (Trust Docs ID: 726)

Information Governance work plan (Trust Docs ID: 16899)

IT Security Policy (Trust Docs ID: 985)

Records Management Information Lifecycle Policy (Trust Docs ID: 7552)

Confidentiality Audit Procedure (Trust Docs ID: 717)

Corporate Records Management (Trust Docs ID: 733)

Cyber Code of Conduct (Trust Docs ID: 982)

Safeguarding Adult Policy (Trust Docs ID: 1105)

Safeguarding Children clinical Guideline (Trust Docs ID: 1179)

Safeguarding Children patient Information leaflet (Trust Docs ID: 10147)

Data Opt-Out policy (Trust Docs ID: 18158)

Policy for Managing Information Governance, Information / Cyber Security Related Incidents (Trust Docs ID: 10008)

Digital Images & Recordings of Patients Policy (Trust Docs ID: 719)

Information Sharing Policy (Trust Docs ID: 8306)

Data Protection Impact Assessment Policy and Procedure (Trust Docs ID: 18157)

Incident Management and Investigation Policy (Trust Docs ID: 15736)

Appendix 1- Caldicott Principles

Principle 1: Justify the purpose(s) for using confidential information. Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary. Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information. Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis. Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities. Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law. Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Appendix 2 - Data Protection Principles and its applications

Data Protection 2018 Principles

There are six principles of good practice for promoting privacy within Article 5 of the General Data Protection Regulation (GDPR) and the data protection Act 2018. These are also underpinned by the principle of **Accountability**, with Article 5(2) stating that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles".

<u>Principle 1 – Processed lawfully, fairly and in a transparent manner in relation to individuals</u>

Fair Obtaining/Consent

There is a requirement to make the general public, who may use the services of the Trust, aware of why the Trust needs information about them, how this is used and to whom it may be disclosed.

This requires The Trust to make reasonable efforts to ensure patients understand how their information is to be used to support their healthcare and that they have no objections.

Where staff are not able to answer a patient's queries on how their information is used, they should be referred to either the Trust's Patient Advisory Liaison Service (PALS) or the Trusts Head of Information Governance.

Patients
Patients will be made aware of this requirement by the use 'Your Information, your rights' Leaflet and will be verbally informed by those health care professionals providing care and treatment.

Staff
Staff will be made aware of this requirement through the staff Privacy notice on the internet and Intranet.

Principle 2 – Purpose Limitation
Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Notification
All databases which hold and/or process personal information about living individuals must be registered with the Trust's Information Governance Team through the Data Processing Activities Tools.

The Trust also need to advise the Information Commissioner's Office (ICO) that is processing personal information.

The Trust is required to maintain records of all these processing activities, which must be made available to Information Commissioner upon request.

For the purposes of Data Protection, a database is considered to be any collection of personal information (more than 51 records) that can be processed by automated means e.g.

Patient records (names and addresses etc.) for appointments

Patient details used for prescribing drugs

Patient information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held on a spreadsheet or access database locally.

Staff records held on Excel to monitor annual leave and sickness, etc.

When collecting personal information, it is essential that the data subject is clear about why the information is being collected and what the information is to be used for. The same information can be used for several different purposes as long as the data subject has been made aware of all of these purposes.

Most the processing done by the Trust will not use consent as its legal basis for the Provision of Health and Social Care.

Consent must be obtained from the data subject if the information collected needs to be used for a different purpose.

Principle 3 – Data Minimisation (Adequate, Relevant and not Excessive)

The Trust must only process the personal data that they need to achieve its processing purposes. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimisation makes it easier to keep data accurate and up to date.

The Data Protection Legislations do not define adequate, relevant and limited. Clearly, though, this will depend on the specified purpose for collecting and using the personal data. It may also differ from one individual to another.

So, to assess whether you are holding the right amount of personal data, you must first be clear about why you need it.

For special category data or criminal offence data, it is particularly important to make sure you collect and retain only the minimum amount of information.

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. You should in particular consider any specific factors that an individual brings to your attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes, and delete anything you no longer need.

When could we be processing too much personal data?

You would be processing too much personal data if you have more personal data than you need to achieve your purpose or when you have included data that are not relevant. You must not collect personal data on the off-chance that it might be useful in the future but cater only for what is required NOW.

If you are holding more data than is actually necessary for your purpose, this is likely to be unlawful (as most of the lawful bases have a necessity element) as well as a breach

of the data minimisation principle. Individuals will also have the right to erasure if they became aware of the excessive information through Subject Access Request.

When could we be processing inadequate personal data?
If the processing you carry out is not helping you to achieve your purpose then the personal data you have is probably inadequate. You should not process personal data if it is insufficient for its intended purpose.

In this case you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question.

How can you practise Data Minimisation?
When collecting data, remember to ask yourself several questions for each point of data you are planning to collect:

1. Does the individual know I am collecting the data?
2. How am I planning to use this data?
3. Does the individual know why I am collecting the data?
4. Is there a way of achieving this purpose without having to collect the data?
5. .How long will I need the data for to achieve the purpose?

Asking yourself these questions will help you understand what data you do and don't need at any one stage, and therefore what data can be erased.

Principle 4 – Accuracy
Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Personal data collected from individuals (Data Subjects) must be complete, accurate and kept up to date – this is similar to the DPA Act 1998 principles. Inaccurate or outdated data should be deleted or amended and data controllers are required to take "every reasonable step" to comply with this principle.

Users of software will be responsible for the quality (i.e. Accuracy, Timeliness, and Completeness) of the data held in their software/systems and must carry out quality assurance audits.

Whenever we speak to a patient over the phone or when a patient visits the Hospital the patient's demographic details must be checked and updated if necessary, by the first member of staff in contact with the patient.

Staff information should also be checked for accuracy on a regular basis. Staff members are responsible for updating their record on the ESR self-service portal.

There may be instances when non-current information needs to be retained e.g. for audit purposes or historical research, where this is the case, the information must be correct at the time it was recorded.

Principle 5 – Storage Limitation

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

All records containing personal information must only be stored for the appropriate length of time. The "NHX Records Management: NHS Code of Practice" provides comprehensive guidance for NHS organisations on the retention period for all NHS records.

The Trust has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and Trust business. It is important this information is disposed of in a secure manner.

Further details of how this affects the Trust, and actions required complying with it, are detailed in the Trust's Records Management Policies, including the Data Retention and Disposal Policies.

Principle 6 – Integrity and Confidentiality

Personal information is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Under the new Data Protection Legislation, personal data must be protected against unauthorised access using appropriate organisational and technical measures. The Trust and its data processors need to assess risk, implement appropriate security for the data concerned and, crucially, check on a regular basis that it is up to date and working effectively.

There are strict breaches reporting provisions in the new legislation. High profile data breaches can cause significant embarrassment and expense for businesses. TalkTalk was recently fined a record £400,000 for failing to keep data secure and this amount will look insignificant if they were to be fined under the new regime of GDPR - up to 4% of annual global turnover or 20m Euros, whichever is higher.

All information relating to identifiable individuals must be kept secure at all times. The Trust will implement policies/procedures to protect Trust information against unauthorised processing of information, accidental loss, destruction and damage to this information. Measures being undertaken are:

All removal media will be encrypted

All laptops will be encrypted.

All software and data is removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is removed from the Trust.

Confidential paper waste is shredded or is collected disposed in the confidential bin ('Blue Bin') the confidential waste bins are kept in safe haven areas and are to be removed by authorised staff only.

Staff will not share user names and passwords.

Trust will implement systems that have appropriate security measures and functionality.

Appendix 3 - Guidance on the Disclosure of Personal Information to the Police, Probation Services and Social & Care

20. Introduction

It is the policy of the Norfolk & Norwich University Hospital NHS Foundation Trust to share legitimate information with the Police, and other services (third party) in a lawful, fair and justifiable way which primarily upholds the service user's right to privacy and confidentiality but releases sufficient, appropriate information to assist the Police with their enquiries, where there is an overriding justifiable purpose (reason) and legal basis to set aside the services users rights to privacy and confidentiality .

A 'third party' is someone who is different from the Trust, or its members of staff authorised to process confidential information

.

According to Article 4 (10) of the GDPR, a third party is "a natural or legal person, public authority, agency or body other than the data subject (e.g. patient or staff member etc.), controller (i.e. the Trust), processor (e.g. supplier contracted to the Trust to process personal data) and persons who, under the direct authority of the controller or processor (e.g. staff member), are authorised to process personal data".

Under the Data Protection Law and Confidentiality: NHS Code of Practice you are under a legal obligation to keep personal information relating to patients and staff confidential and secure.

Information that is provided to the Police by application of this policy is protected from further disclosure to another third party without prior permission being granted by Norfolk & Norwich University Hospital NHS Foundation Trust.

It is a fundamental principle of medical ethics that all that passes between a patient and a doctor/practitioner in the course of a professional relationship is confidential. Patients have the right to expect that information gained in the course of their treatment and care is given to no-one except those involved in their direct care and, even then, only pertinent information is communicated.

For further information relating to processing and sharing information relating to patients – see the Trust Privacy Notice

If in any doubt about disclosure, contact your Departmental Manager, or in the case of a patient, the Duty Hospital Manager or On Call Consultant or the Head of Information Governance - Data Protection Officer.

21. General issues

In general, disclosure of personal data should not be made to unauthorised third parties, including family members, friends, government bodies and, in certain circumstances, the Police. ”This means no member of staff should disclose information about another person to a third party, other than for good, duly considered reasons that can be justified as lawful.

If staff are in doubt, they should seek advice in the first instance from their Team/Line Manager. If further advice is required – please contact the Information Governance Team on 01603 289595 info.gov@nnuh.nhs.ukt.

Child Protection

In Child Protection matters, Locality Safeguarding Children Boards (LCSBs), Child Protection Procedures and Hospital Child Protection Policy should also be followed. Advice should be sought from the Safeguarding Team.

If you suspect a child is being abused, but there is no request for information, you have a legal power to disclose information to Children’s Services (Children’s Act 1984, under ‘vital interest’ conditions of the Data Protection Law and or the Police under the Police and Criminal Evidence Act). Consider whether obtaining consent from the child or the parent would be beneficial or detrimental to the situation. If detrimental then you should disclose without gaining consent.

Always inform the Trusts Named Nurse for Safeguarding Children prior to disclosing information relating to Children.

Vulnerable Adults

Where issues relate to vulnerable adults, for further help, advice and guidance on disclosing information concerning a “Vulnerable Person” refer to the “Safeguarding Adult Policy”.

Always inform the Trust’s Named Nurse for Safeguarding Adults prior to disclosing information relating to a vulnerable person.

Only give the minimum relevant, information, to satisfy the request: there is a difference between disclosing specific information about an individual and releasing copies of all the contents of staff personal record or patient’s medical record. The golden rule is for both the Trust and the Police to be able to justify the release of information being in the public interest.

In all cases of requests that may involve a third party the Patient Access Coordinator must be informed, and the request to disclose information must be recorded on the SAR log, with reasons for action taken, e.g. why information was given or withheld.

22. Procedure to be followed – (see Appendix 3a for decision flow diagram)

Seek assistance

When a member of staff receives a request for patient/staff information from the Police, they should contact their Team Manager, and if out of hours, the Senior Clinician or Manager on Call.

Validate the request:

A Police officer, wishing to make enquiries into the case of a serious offence, should ask to see the Clinician or Manager of the department responsible for the care of the patient (who is suspected of involvement in the offences under investigation, either as a victim or perpetrator). The genuine identity of the person representing themselves as a Police officer must be established (e.g. warrant card examined).

Requests from the Police to access clinical records, must always be made in writing. Such requests can be made under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018– Ask for an authorised request.

Where Police attend Trust premises in response to an incident involving a patient, the Police officer will normally ask the medical staff to determine whether the person is fit to be interviewed. It is generally considered appropriate, ideally with the patient's consent. The Police officer will often ask staff whether the patient knew what they were doing and whether they were responsible for their actions. In these cases the doctor should not give information without the express consent of the patient.

Obtain Consent:

Where possible, practical, and safe to do so, the patient's consent to release information should be obtained by the Trust. However, there may be times when this is not possible due to the patient's condition, for example the patient does not have capacity to consent and will not gain capacity to consent in a timely manner; is unconscious or has absconded, or has been discharged from the care of the Trust, or where gaining consent is likely to result in further incidents or risk. The duty of care also requires the Trust to consider whether the patient is capable of making an informed decision.

Disclosure of information to the Police without the patient's Consent:

The consultant or lead healthcare professional involved with the patient, or their deputy, has discretion, within the law, over what information may be given to the Police (whether in writing or following attendance by a Police officer to his or her Department). Where Police attend outpatient clinics, there may not always be a designated consultant with responsibility; in these cases the senior clinician will need to make the decision.

If a health professional is considering disclosing health records without consent, the records should be reviewed by the clinician in charge of the patients care. A discussion with colleagues should take into account the following factors:

Damage to the relationship between the health professional and the patient.

Impact of the patient ending the relationship

Risk of breakdown of trust between the patient and the NHS

Risk of loss of confidence amongst the public as to the confidentiality of the NHS services.

Whether this is compliant with statutory legislation (for example the Data Protection Act 2018)

The reasons for and against disclosure

Likely risks of litigation for any potential breach of confidentiality.

If a decision is made to disclose without consent, the information should be given to the most appropriate accountable person to minimise the impact on the individual. Consideration should be given to whether the recipient is likely to disclose the information further and whether it is appropriate to place conditions of disclosure to limit any damage.

Circumstances where information may be released (patient/staff) – Statutory Obligations

There are some specific circumstances in which there are statutory requirements to assist the police. The third party e.g. the police must be asked to state under which specific legislation disclosure of information is sought. Unless a court order is secured, or legislation explicitly requires disclosure, the decision to disclose remains with the Trust.

If such legislation exists, the onus is on the requester to provide a full and accurate citation in order for us to be satisfied the disclosure is lawful. All citations must be fully checked – we have experience of inaccurate citations being made to attempt to get information disclosed unlawfully.

Citations of the Data Protection Act itself are not valid justification on which to base disclosure.

Examples (and this is not exhaustive) of statutory disclosures where health professionals are required by law to disclose to police are:

a. If the public interest and safety out-weighs the duty of confidentiality; this is likely to involve crimes of a very serious nature or where a serious offence is being investigated, such as rape, murder, kidnapping, causing death by dangerous driving or fire-arm related crimes.

b. if information relating to terrorism has been acquired;

c. If the provisions of Section 172 of the Road Traffic Act 1988 apply (name and address). Where the investigation concerns offences involving motor vehicles staff can provide the Police with patient/occupant/driver demographic details. Under Section 168 (2) (b) of the 1972 Road Traffic Act any person (e.g. Trust staff) must give information that may lead to the identification of the driver of a vehicle, where the driver is alleged to have committed an offence under the Act. It should be noted that the information is restricted only to enable an identification of the driver and no other information should be given. (Hunter-v-Mann 1974). The Police Officer should not be permitted to examine any medical or nursing notes or any record books or administration books kept in the hospital. If unsure seek advice.

d. If the release is for the prevention and detection of crime and is a life or death matter and the decision has been made that its release is 'in the public interest and safety' then the appropriate information must be released and the Trust's Health Records Manager informed. The Police must provide a completed and signed DP2 form (see 3.2).

e. Where public interest context to furnish certain information about a patient/staff to the Police over-rides the duty of confidentiality. i.e. there is sufficient public interest justification to release it.

f. Where it is evident to staff that they, colleagues or members of the public may be at risk of harm and that involving the Police or other agencies is appropriate.

   The Caldicott Guardian, Data Protection Officer or senior managers agreement must always be obtained whenever possible. Examples include detained patients who are absent without leave or patients who are registered as missing persons.

g. If a Court Order has been obtained.

In all cases, the authority of the Consultant or Senior Clinician in charge of the patient must be obtained.

Release of information to the Police in authorised Police break-ins or missing person cases

The Trust should always seek to determine why the Police need the information, and what legal bases is to be relied upon.

There are certain emergency situations where the Police will ask, by phone, if an individual is an in-patient for example. In these cases, staff should ask for the name and rank of the officer and call the station back using the telephone number obtained from switchboard. Information may only be disclosed if it can be justified to be in the public interest, e.g. risk of serious harm or death.

There are occasions when the Police contact the hospital seeking information about missing people. Such enquiries should not be made by telephone but by a visit to the hospital or by a written request. If it is an emergency, then the above paragraph applies.

There may be situations where Police enquire as to whether someone about whom they have received reports and/or are about to engage with is known to the Trust. In these cases, the same tests apply as above with the over-riding test being consideration of the patient's privacy and confidentiality and the lawful justification for overriding and setting aside a patient's privacy and confidentiality. The following are given by way of examples (and it is not exhaustive) where release of information may be appropriate:

Police have received a report about a person acting in a bizarre way. Police attend and believe the behaviour may be the result of a mental illness and wish to test if that person is known to us so that they can ensure appropriate treatment;

In missing person cases, where the Trust knows the patient is in hospital, the Trust should ask the patient for their consent to pass the information on. If the patient does not want the information passed on (for example to relatives) then the Police should be told this. A record of the request and the outcome must be placed in the health record;

Where the patient is not in a position to give/withhold informed consent and it is seen to be in the patient's best interest to give information (e.g. the patient does not have the capacity to consent or is unconscious in intensive care unit) then information should be released based on a professional judgement/justification. Again, a record must be made in the health records. In such circumstances appropriate authorisation should be sought from a Senior Clinician, Senior Manager or Caldicott Guardian whenever possible.

Where Trust staff approach the Police

In certain areas of the Trust's work it is recognised staff are at risk of crime from patients, relatives and the public. They may also come across evidence of serious crime. All staff have the same rights and duties as any other citizen, and the Trust also has a duty not to infringe or diminish those rights or duties. The Trust recognises, in certain circumstances, involving the Police may be the appropriate way of dealing with a situation or its consequences.

In some circumstances staff will come across evidence of serious crime, for example; the possession of firearms or other weapons or drugs. Where this occurs on Trust property (e.g. as part of admission procedures) the Police should be informed. Please refer to the Trust's 'Search of Patients and their Property Policy' for full guidance. All such incidents (whether on Trust property or not) must be reported.

In addition to the above, Trust staff need to bear in mind the nature and circumstances of the patient's injuries and the possibility that they may indicate involvement in serious crime, for example, terrorism, violent battery, murder or the production of explosives. In view of anti-terrorist legislation measures, these instances must be notified to the Police immediately after seeking advice from the appropriate manager.

Multi Agency Public Protection (includes the Probation Service)

The Criminal Justice and Court Services Act 2000, sets the framework for sharing information about potentially dangerous offenders. Information about individuals may be required by 'Multi Agency Risk Conferences'. If you are requested to provide

information, you should consider gaining consent/informing the individual(s) unless this may cause more harm than good. If the risk presented by an individual(s) clearly cannot be effectively managed without information and gaining consent is inadvisable, then relevant information can be shared as it is in the interests of the public.

Multi Agency Risk Assessment Conference – MARAC Operating Guide
The MARAC is an integral part of the Coordinated Community Response model to Domestic Abuse in Norfolk. It is linked to the Independent Domestic Violence Advocacy (IDVA) service and the Specialist Domestic Violence Court (SDVC). The Trust has signed an information Sharing Agreement with the Norfolk Partners.

Domestic violence is multi-faceted and complex; there are overlaps with services being delivered and impacts on all involved i.e. the victim, perpetrator and child (if there are children involved). Agencies cannot deal with, and provide an effective service to victims and their children as well as the management of perpetrators alone.

Therefore, under this information sharing agreement as the legal basis, The Trust will disclose information about the victims, perpetrators and child (if there are any children involved) to reduce the risk of harm or homicide for a victim and their families and to increase the safety, health and wellbeing of the victims.

Refusal to disclose
There may be circumstances when a health team decide not to disclose patient information. It is essential that whatever decision is taken, the health professional can justify the decision and has clearly documented the process of decision making. The police may seek an order from a judge or a warrant for the disclosure of confidential documents. The decision making process and documentation around this will be helpful in feeding into any court process.

If sending the information electronically, make sure they are encrypted to the minimum required Doha standard AES 256 Bit or alternatively if sending by email, ensure the transmission is secured e.g. *.nhs.net to *.pan*(police secure network). If staff need to send an encrypted email please call the IT Service Desk or log an IT Service Desk call.

Appendix 3a – Decision Flow Diagram

Appendix 4 – Telephone Guidance for handling calls where Personal Identifiable Information may be disclosed.

Receiving and making calls:

Health information is legally defined as 'sensitive'. There are many examples where information has been given to an inappropriate person or in extreme circumstances impostors have been able to obtain sensitive patient information. Not everybody has an automatic right to know about someone else's medical or health condition, whether they are family, friend, carer or health professional. The health information can be disclosed only if the patient/staff has consented for these to be disclosed.

General guidance

Wherever possible, do not make calls where you can be overheard, especially by members of the public.

As part of general discussion with patients, you should make them aware of what information you may need to discuss with others caring for them – 'implied consent'.

If a patient raises concerns about telling other people, do your best to respect that, especially when talking to their relatives/friends or others. Make sure it is documented in the medical records. Take some time to explain the consequences for not disclosing their information to others who are caring for them.

Calls to/from staff involved in care of patients

Always confirm who you are speaking to before releasing information. If someone has called you and you are not sure who they are, ask for a number to ring back, usually via the switchboard. Always check the number whether it is listed on the Patient Administration System. If not confirm with the patient if they recognise this number.

For patients who have a long stay in the hospital, set a password/pin with a close family member/Carer whom the patient has consented to receive their personal data or someone who has the lasting power of attorney. In those circumstances, the identity can be checked using the pin.

If you can't call them back, because time or circumstance don't allow, don't be afraid to ask questions of them. Information should only be disclosed to those who can prove they need to know. 'Because I am….' is not a sufficient reason. A bona fide requestor should not be concerned about answering questions.

If you know the patient is unable to speak to you, or the recipient of the call tells you that they effectively act on the patient's behalf which could be verified on the system, then you can pass limited information to the recipient.

Health professionals and carers may need to know information to provide best care for the patient, hopefully you have their 'implied consent' (see general guidance above) but you may need to provide it without consent in circumstances that warrant it, the key is to document your decision making process.

Calls to/from relatives/friends/others
Confirm information, ask the caller to provide information about the patient or request the pin number if you have one set up, to confirm you are talking about the right person. This might discourage some 'bogus' callers as well as confirm you have the right person's information. Some typical questions/answers would be:

Who is the caller? What is the relationship to the patient? Why do they need to know? Has the patient expressed whether they should or shouldn't be told?

'Can you tell me how 'X' is?' – Unless you have patient consent, or can justify why the caller should know, then very limited information should be given out.

'Can you tell me what time/date 'X's appointment is?' –, are they acting on behalf of someone who can't check for themselves? Do you have a record of who made the appointment? (If a young person made their own appointment, is it because they don't want their parents involved at present?)

'Has 'X'D' finished at the Doctors?' – Ask 'what time was their appointment?' 'Who were they seeing?'

When calling someone at the request of the patient, or because they need to be contacted always try to speak directly to the individual without releasing information to whoever answers the phone if at all possible.

Leaving messages on Answerphones:
Patient confidentiality can be breached from messages left on answer phones, resulting in embarrassing, distressful or harmful situations arising. The following points offer guidance about this.

Before leaving a message consider the urgency of getting the information to the patient. If it is not urgent and another attempt to speak to the patient can be made, do not leave a message.

If you feel you have to leave a message, think about what you say, and leave the minimum amount of information – for example, 'Please call (number) to talk about your appointment' (This will be clear to the patient, but ambiguous to anyone else hearing the message.)

Do not leave messages like this real example 'The bad news is you have cancer, the good news is it is small…'

When the phone is answered by someone else:

1. Always ask to speak to the patient, but don't say where you are calling from initially.
2. If they ask who is calling, you should respond with a minimum amount of information. Stating you are calling about their appointment may be sufficient. If they continue to ask where you are calling from, only tell them the organisation name and not the department name.
3. If the patient is not present, then unless there is a degree of urgency do not leave a message, but ask when a good time to call back is.
4. If the patient is present but unable to speak (either due to language or physical difficulties), ask to speak to the next of kin. Before giving information to them, try to ascertain whether they are aware of why you may be calling (it may be necessary to reveal basic information to do this)

This guide cannot be comprehensive about what is a complex area, as there are many case by case factors (patient mental capacity, implied consent etc.) which may make a difference. The key really is to take a moment to think about:

Who are you talking to?

What information do they want? How much is really needed?

Why do they need it?

What impact might disclosing information have? Even if it seems basic, there have been issues relating to telling people about attendance etc.

Appendix 5 – Application of the Data Protection Act in relation to the employment Practice Code.

Reference is made to the Data Protection - Employment Practices Code

Data protection compliance should be seen as an integral part of employment practice. It is important to develop a culture in which respect for private life, data protection, security and confidentiality of personal information is seen as the norm.

This guidance covers all aspects of the collection, holding and use of employment records from the initial obtaining of information once a worker has been employed or engaged through to the ultimate deletion of the former staff member's record. It also deals with the rights of job applicants as well as staff members to access to information the employer keeps about them.

23. Recruitment and Selection and the Data Protection Law

If the Trust collect or use information about people as part of a recruitment or selection exercise, the Data Protection Law will apply. For example, personal information about people will be obtained by asking them to complete an application form or to e-mail their CV to you.

The Act requires openness. Applicants should be aware what information about them is being collected and what it will be used for.

a. Things to remember when collecting or using information about Job Applicants

The Trust names and details should always be mentioned when advertising for the job or the agency/third party details, if they are being used.

Use the information you collect for recruitment or selection only. Any other purpose would require consent from the applicants.

Ensure that those involved in recruitment and selection are aware of data protection rules and that they must handle personal information confidentially.

Do not collect excessive or irrelevant personal information than you need and design the application form bearing this in mind.

Do not collect from all applicants' information that you only need from the person that you going to appoint, such as banking details, Emergency contact.

Keep the personal information you obtain secure and accessible by authorised staff ONLY.

Only ask for information about criminal convictions if this is justified by the type of job.

If you are going to verify the information a person provides, make sure they are aware of that.

If you need to verify criminal conviction information, only do this by getting a 'disclosure' about someone from the Criminal Records Bureau (CRB). Only keep a record that a satisfactory/unsatisfactory check was made; do not hold on to detailed information.

Only keep information obtained through a recruitment exercise for as long as there is a clear business need for it.

24. Employment Records

The Data Protection Law:-

WILL apply to information you keep about your staff

DOES NOT prevent you from collecting, maintaining and using employment records. However, it helps to strike a balance between the employer's need to keep records and the staff member's right to respect for their private life

REQUIRES OPENNESS. Staff members should be aware what information about them is kept and what it will be used for. Gathering information about a worker covertly is unlikely to be justified.

a. Things to remember when collecting, keeping and using information about your staff members:-

The Trust do not require the consent of staff members to keep records about them, but make sure they know how the Trust will use records about them and whether it will disclose the information.

Ensure that those who have access to employment records are aware that data

protection rules apply and that personal information must be handled with respect.

Check what records are kept about staff members, and make sure you are not keeping information that is irrelevant, excessive or out of date. Delete information that you have no genuine business need for or legal duty to keep.

Before disclosing the staff employment record, always seek confirmation of his/her identify and purpose as why this information is required.

Data protection doesn't stand in the way where you are legally obliged to disclose information, for example informing the Inland Revenue about payments to staff members.

In some cases The Trust will not be legally obliged, e.g. criminal or tax investigations or legal action, to disclose but most of the time an exemption in the Data Protection Act if you choose to do so.

Only disclose if, in all the circumstances, you are satisfied that it is fair to do so bearing in mind that fairness to the staff member should be the first consideration.

Don't provide a confidential reference or similar information about a staff member unless you are sure that individual has been made aware of the request. If in doubt, ask the individual concerned.

Let staff members check their own records periodically. This will allow mistakes to be corrected and information to be kept up to date.

Keep employment records secure. Keep paper records under lock and key and use password protection for computerised ones. Make sure only staff with proper authorisation and the necessary training have access to employment records.

Where possible, keep detailed sickness records separate from other less sensitive information, for example a simple record of absence.

If you collect sensitive information to help monitor equal opportunities, for example about staff members' disabilities, race or sexuality, only use the information for that purpose. Where possible use anonymised information, information that does not allow particular staff members to be identified.

If you intend to use the information you keep about staff members to send marketing material give them a chance to opt out before doing so.

If you intend to pass on their details to another organisation for its marketing, then get the staff member's consent before doing so(opt-in rather than opt-out).

Dispose of these records securely by following Trust policy and NHS Records Management Code of Practice when you no longer have a business need or legal requirement to keep that record.

25. What rights do Staff members have? - Subject Access Request

Under the Data Protection Act, staff members have a legal right of access to information the Trust hold about them. This includes information about grievance and disciplinary issues, and information you obtain through monitoring.

Make sure you have arrangements in place to deal with access requests appropriately and within the 40-day time limit stipulated in the Data Protection Act.

When giving access to employment records be careful with third party information. It could be wrong, for example, to disclose the identity of someone alleging harassment to the person accused of carrying out the harassment.

Disclosure should be done in accordance with the Subject Access Request Code of Practice.

26. Monitoring at work

If you monitor your staff members by collecting or using information about them, the Data Protection Act will apply. This can happen, for example, when you video staff members to detect crime, when you check telephone logs to detect excessive private use, and when you monitor e-mails or check internet use.

The Act requires openness therefore staff members should be aware of the nature, extent and reasons for any monitoring unless, exceptionally, covert monitoring is justified.

The Act doesn't prevent monitoring but sets out principles for the gathering and use of personal information. In short, data protection means that if monitoring has any adverse effect on staff members, this must be justified by its benefit to the employer or others.

a. Points to consider when monitoring

The reason why you want to carry out the monitoring bearing in mind that:

1. Monitoring is usually intrusive.
2. Staff members legitimately expect to keep their personal lives private.
3. Staff members are entitled to some privacy in the work environment.

Once you are clear about the purpose, ask whether the particular monitoring arrangement will truly bring the benefit you are looking for and whether it is justified by this benefit. Keep staff members informed of the process.

You could tell them by putting a notice on a notice-board or signs in the areas where monitoring is taking place. If your staff members have access to Trust emails you could send them an e-mail about the monitoring. If you are open about it, they will know what to expect.

If monitoring is to be used to enforce your rules and standards, make sure staff members know clearly what these are.

Only use information obtained through monitoring for the purpose for which you carried out the monitoring, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore, for example breaches of health and safety rules that put other staff members at risk.

Keep the information that you gather through monitoring secured at all time. This might mean only allowing one or two people to have access to it. Don't keep the information for longer than necessary or keep more information than you really need. This might

mean deleting it once disciplinary action against a worker is over.

b. Covert/Secret monitoring

The covert monitoring of staff members can rarely be justified.

Do not carry it out unless it has been authorised by the Chief Executive Officer.

Use covert monitoring only as part of a specific investigation, and stop when the investigation has been completed. Do not use covert monitoring in places such as toilets or private offices unless you suspect serious crime.

27. Safekeeping and Storage of employment records

All personnel file should be treated as confidential and handled according in line with the Data Protection principles, Caldicott principles and the NHS, Confidentiality Code of Conduct see Appendix 1.

All personal files must be kept in a lockable cabinet, which is kept locked at all times when not in use.

Access is to be restricted to managers only, who should hold the keys to the cabinet.

Access might also be granted to other named individuals, such as the Manager's Assistant, Secretary or Deputy, when there is a business need for this access.

Information from an individual's personal file should not be disclosed to a third party without the consent of the employee unless the third party is in a direct line management relationship with the individual.

For further guidance contact the ICO website for the full code of practice: Data Protection - Employment Practices Code

Appendix 6 – Task of a Data Protection Officer

Art. 39 GDPR - Tasks of the Data Protection Officer

The data protection officer shall have at least the following tasks:

28. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
29. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
30. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
31. To cooperate with the supervisory authority;

32. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.