Trust-wide Policy
Information Governance Policy

Policy number:	Corp - 00263
Scope of policy:	All staff
Ratifying committee:	Information Governance Steering Group
Date ratified:	09 August 2024
Next review date:	09 August 2027
Date implemented:	09 September 2024
Accountable lead job title:	Senior Information Risk Owner
Division and/or department:	Corporate / IT
Lead author(s) job title:	Head of Information Governance / Data Protection Officer
Document summary:	Overarching Policy covering data protection, data security and confidentiality in the Trust. Includes the Code of Best Practice for Employees in Respect of Confidentiality (Appendix G).
Published by:	Corporate Governance Team, Great Western Hospitals NHS FT
To be read in conjunction with:	• The common law duty of confidentiality/confidence (Ref 1) • The Caldicott principles (Ref 2) • Data Protection Act 2018 (DPA) (Ref 3) and the General Data Protection Regulation (GDPR) (Ref 4) (as enacted by the EU (Withdrawal) Act 2018 [ref 31] and subsequent regulations) • Freedom of Information Act 2000 (FOI) (Ref 5) • Data Protection Policy (Ref 7) • Records Management Code of Practice for Health and Social Care (Ref 28)
Review period:	This document will be fully reviewed every three years in accordance with the Trust's agreed process for reviewing Trust-wide documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.

Version control history
Please record brief details of the changes made alongside the next version number.

Version	Brief summary of changes
4.0	List of possible offences added as an appendix. Added additional text to IG training, staff responsibilities, pseudonymisation/anonymisation and national data opt out sections for clarity. Also reviewed by SFT IG colleagues to support alignment.

Contents

1) Purpose and rationale

Purpose:

Information (both electronic and manual), and the systems it is held within, are a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. They play a key part in governance, service planning and performance management. The security of information is therefore paramount and can be underpinned by ensuring its:

Confidentiality – information must only be accessed by those authorised to do so

Integrity – information must be complete and accurate. All systems, assets and networks must operate correctly, according to specification

Availability – information must be available and delivered to the right person, at the time when it is needed.

To fully understand the requirements of IG, the full catalogue of IG policies should be read in conjunction with this policy. These are listed in Section 9 of this document.

2) Scope

This document applies to all staff employed by The Great Western Hospitals NHS Foundation Trust (whether on a permanent, temporary or honorary contract) who are involved in writing, reviewing or managing policy documents.

3) Definitions

The following terms and acronyms are used within this document:

CD	Compact Disc
CQC	Care Quality Commission
Data Subject	Any person whose personal data is being collected, held or processed.
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DSCRO	Data Services for Commissioners Regional Office
DSPT	Data Security and Protection Toolkit
DVD	Digital Versatile Disc
EIA	Equality Impact Assessment
EPA	Enduring Power of Attorney
ESR	Electronic Staff Record
EU	European Union
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
GMC	General Medical Council
GP	General Practitioner
ICB	Integrated Care Board
ICO	Information Commissioner's Office
IG	Information Governance
IGSG	Information Governance Steering Group
IT	Information Technology
LPA	Lasting Power of Attorney
LPA / EPA	Lasting Power of Attorney / Enduring Power of Attorney
NCRS	National Care Records Service

NHS	National Health Service
NMC	Nursing & Midwifery Council
PBAC/RBAC	Person-based or Role-based Access Control
PC	Personal Computer
PHSO	Public Health Service Ombudsman
SAR	Subject Access Requests
SIRO	Senior Information Risk Owner
TNA	Training Needs Analysis
UK	United Kingdom
USB	Universal Serial Bus

4) Duties

4.1 Chief Executive

The Chief Executive is ultimately responsible for the implementation of this document.

4.2 Ward Managers, Matrons and Managers for Non-Clinical Services

All Ward Managers, Matrons and Managers for Non-Clinical Services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

4.3 Document Author and Document Implementation Lead

The document Author and the document Implementation Lead are responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

4.4 SIRO (Senior Information Risk Owner)

The SIRO is accountable for information risk within the Trust and advises the Board on the effectiveness of Information Risk Management across the organisation, including the logging and monitoring of key information risks on the corporate Risk Register.

The SIRO shall:

- be accountable for the management and protection of all Information Assets;
- lead on Business Continuity in the context of Information Risk;
- provide senior line management to the IG and Digital (including cyber security) teams;
- act as Executive lead for the IG Framework;
- advise the Board on the effectiveness of IG and Cyber assurance across the Trust;
- review and sign off the annual Data Security and Protection Toolkit assessment;
- approve and appoint Information Asset Owners (IAOs);

4.5 Caldicott Guardian

The Caldicott Guardian is an advisory role and acts as the “conscience” of an organisation, actively supporting work to facilitate and enable information sharing, and advising on options for lawful and ethical processing of information as required. The Caldicott Guardian reflects the priorities of the National Data Guardian (NDG) and is particularly concerned with the management of patient information, ensuring that it is safeguarded securely and used properly.

The Guardian shall:

- ensure that the Trust satisfies the highest practical standards for handling patient identifiable information;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion IG requirements and issues at board level;
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for Employees;
- be the signatory to information sharing protocols and agreements with partner organisations where confidential patient information needs to be shared across organisational boundaries;
- be the decision-maker for complex queries or situations where the use or sharing of data may need to be done without consent or where it is done in the best interests of a person or persons, where some parties may disagree with the sharing;
- provide a focal point for patient confidentiality and information sharing issues.

4.6 DPO (Data Protection Officer)

The Data Protection Officer (DPO) is responsible for ensuring that the Trust and its constituent business areas remain compliant at all times with various Data Protection legislation, NHS codes of practice and common law duties.

The DPO shall:

- be the Trust's first point of contact for the Information Commissioners Office (ICO)
- inform and advise the organisation and its Employees about their obligations to comply with the GDPR and other data protection laws;
- manage internal data protection activities, such as advising on data protection impact assessments; training Employees and conducting internal audits;
- ensure information for patients and staff is published in relation to how their information is held, used and shared, and answering queries in relation to this, including establishing processes for managing objections;
- line manage Freedom of Information (FOI) requests made to the Trust;
- manage IG related incidents on behalf of the SIRO, ensuring the development of actions plans and external reporting where appropriate.

4.7 Employees with Information Governance Responsibilities

Employees with Information Governance (IG) responsibilities must ensure that they remain abreast of current legislation or other guidance e.g. from the Department of Health & Social Care, the UK Council of Caldicott Guardians, the Information Commissioner's Office etc. They must ensure that they have undertaken appropriate training in Information Governance and are confident with assisting other employees to make informed decisions regarding information disclosure

4.8 The IG Steering Group

The IG Steering Group is to ensure that the Trust has effective policies and management arrangements covering all aspects of Information Governance (IG) and to monitor all IG activities and performance.

5) Process

5.1 Key Areas of Information Governance

5.1.1 Common Law Duty of Confidentiality

Patients entrust their personal information to the National Health Service (NHS), or allow the NHS to gather it, as part of their treatment and care. They have a legitimate expectation that Trust employees

will respect their privacy (confidentiality) and act appropriately. This expectation also extends to other personal information that the Trust holds, e.g. about its employees.

All employees of the Trust have a duty of confidentiality; therefore, information must not be accessed or processed unless there is a genuine reason to do so.

The common law duty of confidentiality extends beyond death and therefore the information of individuals that are deceased must still be treated confidentially.

Article 8 of the Human Rights Act 1998 (Ref 6) also emphasises confidentiality and states that individuals have the 'right to privacy and family life' with no interference.

Confidentiality must form the basis of any decision involving an individual's personal information

5.1.2 Caldicott Principles

The Caldicott Principles are a set of eight standards created by the National Data Guardian, that must be met when using or sharing information:

- Principle 1 - Justify the purpose(s) for using confidential information
- Principle 2 - Don't use personal confidential data unless it is absolutely necessary
- Principle 3 - Use the minimum necessary personal confidential data
- Principle 4 - Access to personal confidential data should be on a strict need-to-know basis
- Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities
- Principle 6 - Comply with the law
- Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality
- Principle 8 - Service users must be informed about how their confidential information is used

It is recognised that information is crucial to providing a quality healthcare service. The final two principles encourage information to be used provided the other principles have been met and that there is a lawful basis for processing the data within the DPA/GDPR.

5.1.3 Data Protection Act / UK General Data Protection Regulation

The DPA 2018 and the UK GDPR identify six lawful bases for processing information. These are:

a. Consent
b. Contract
c. Legal obligation
d. Vital interests
e. Public task
f. Legitimate interests

For further information about the DPA and the UK GDPR see the Trust's Data Protection Policy (Ref 7). Appendix B of this document provides guidance on the lawful bases and the rights of data subjects under each one. Appendix C of this document provides guidance on what constitutes valid consent and what to do if the data subject, the person who the information relates to, does not have the capacity to give their consent. Appendix D of this document gives examples of information disclosures.

5.1.4 Freedom of Information

Under the Freedom of Information Act 2000 (FOI) (Ref 5) and the Environmental Information Regulations 2017 (Ref 8) anyone can request information from a public authority. The Trust, as a

public authority has a duty to respond to these requests within statutory timeframes. There are some exemptions to information being provided, for example, section 40 of the FOI Act 2000 (Ref 5) states that personal information is exempt from disclosure. For further information please refer to the Freedom of Information Requests Procedure (Ref 9).

5.1.5 Information Security

Security of information is paramount to protect the privacy of the Trust's patients and employees, and to ensure that the Trust can efficiently perform its duties as a healthcare provider.

Please refer to the Code of Best Practice at Appendix G for guidance on how to manage Information Governance responsibilities. Please also refer to the relevant healthcare regulators guidance, for example the General Medical Council (GMC) Codes of Conduct, Ethics and Confidentiality.

All employees, including temporary staff and volunteers, are responsible for ensuring that breaches of confidentiality or of information security do not result from their actions. The ICO can take action against the Trust, or if the breach was deliberate or seriously negligent, against individuals. Breaches such as inappropriate access or disclosure may result in disciplinary action, a criminal prosecution and/or a fine. Individuals may also be referred to their healthcare regulator if it is deemed that their fitness to practise may be impaired. A list of offences relating to personal data is available at Appendix F – this list is not exhaustive.

Any breach, or suspected breach of confidentiality must be reported on an incident report form, and the Information Governance (IG) team should be informed. Further information is available in the Trust's Data Security & Protection Incident Reporting Procedure (Ref 10). Learning from incidents must be shared with the relevant teams or individuals and actions agreed to prevent the incident from happening again.

5.1.6 Records Management

The Trust complies with the 12 generic record keeping standards approved by the Academy of Medical Royal Colleges. These are listed in the Trust's Clinical Record Keeping Policy (Ref 11).

Retention periods for all types of records are listed in the Records Management Code of Practice 2021 (Ref. 12). This list is also available on the Trust's intranet site. Further information about records retention and disposal may be found in the Trust's Retention of Records Policy. (Ref 13)

5.2 Compliance and Assurance Work Programmes

Each year, the Trust must complete the Data Security and Protection Toolkit (DSPT) [Ref 14] which is managed by NHS Digital. The DSPT assesses compliance with information governance standards throughout the year. The DSPT submission is subject to an internal audit for assurance purposes.

5.3 Employee Training

All employees of the Trust must complete training in information governance at least annually. The online training must be completed in the first year of employment with the Trust and refresher training completed in each subsequent year – which is monitored and recorded based on the DSPT submission dates. IG training forms part of an employee's' mandatory training and compliance must be recorded on annual performance appraisals.

The Academy manages the Electronic Staff Record (ESR) system for employees to use and the IG training modules have also been made available on an online platform to circulate to employees via email, which is managed by the IG team. In addition to this, booklets have been created for employees with little or no computer access. All methods of training consist of key information and a test of

comprehension. A training needs analysis (TNA) has been created to identify role specific training and is approved annually by the IG Steering Group (IGSG).

There is a target of 85% for all employees (including Bank staff and volunteers etc) to complete IG training during the DSPT submission year (July-June). Other staff who manage personal or confidential data more extensively will need to meet a higher compliance target. Compliance is monitored by the IG Team and scrutinised by the IG Steering Group who review progress on achieving compliance on a Trust-wide basis.

5.4 Anonymisation / Pseudonymisation

In accordance with the Data Protection Act and the Caldicott Principles, minimum data should be used at all times, and it should only be accessed on a strict need-to-know basis. Therefore, when using information for purposes other than direct healthcare, data should be altered to protect the privacy of the data subject that it relates to. This can be done by anonymising or pseudonymising the dataset.

Anonymous data has all identifiers removed making it impossible for the data subject to become known or re-identified by any person.

There will often be circumstances where the identity of the data subject does not need to be shared, but it may need to be known by Trust employees or linked with other datasets to provide better analysis. In these circumstances the data should be pseudonymised. This is a process which removes identifiers but retains a unique reference number or code allocated to each data subject. The person pseudonymising the data must store the list of names and numbers securely and not share it and must keep a record of the key to the identifiers used. The recipient of the pseudonymised data would therefore be unable to identify to whom it related to. However, if the person who shared the data needed to re-identify the data subject(s) then they would be able to match the pseudonymised number back to the full details. Some systems will be able to produce pseudonymised lists, as required, to comply with DSPT standards. Where data is rich (multiple data fields), further obscuring of details may be required; for example, using the year of birth or age range instead of the full DOB, or using the first digits of a postcode instead of the whole sequence.

5.5 National Data Opt-Out

The National Data Opt-Out was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes. This is provided in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs. Information on the National Data Opt-Out can be found here: https://www.nhs.uk/your-nhs-data-matters/.

NHS England holds a list of people who have decided to opt out of their information being used for research and planning purposes. When using confidential information for research and planning purposes, health and care organisations are required to apply national data opt-outs by liaising with NHS England who will remove individuals from data sets and return it to the organisation.

The opt-out does not affect data being used for direct care. The opt-out applies to data being used for research or planning purposes unless there is a mandatory legal requirement or an overriding public interest for the data to be shared; for example, responding in a pandemic. Anyone that has opted out, can subsequently provide consent for individual uses; for example, a research project they wish to participate in. The opt-out does not apply to anonymous datasets.

A flowchart is available at Appendix E.

5.6 Incident Reporting

If a data security and protection incident occurs, whether accidental or deliberate, this must be reported on the Trust's Incident Reporting System (Ref 13). Reporting these types of incident leads to a greater awareness of potential risks or concerns and gives the Trust an opportunity to take action to prevent incidents recurring.

If an employee becomes aware of a data security and protection incident, they must consult the IG team as soon as possible as serious incidents must be reported to statutory bodies, including the Information Commissioner's Office (ICO), within 72 hours of the incident occurring.

Further information is available in the Trust's Data Security & Protection Incident Reporting Procedure (Ref 10).

6) Consultation

Below is a list of consultees who supported the formulating of this document.

Job title and department	Date approved
Head of IG and DPO	14 July 2024
Deputy IG Manager (SFT)	18 July 2024
Deputy IG Manager (GWH)	23 July 2024
IG Officer (GWH)	23 July 2024
IG Steering Group	09 August 2024

7) Training and support

See Section 5.3 of this document.

8) Monitoring, compliance, and effectiveness of implementation

The arrangements for monitoring compliance are outlined in the table below:

Measurable policy objectives	Monitoring or audit method	Monitoring responsibility (individual, group or committee)	Frequency of monitoring	Reporting arrangements (committee or group the monitoring results is presented to)	What action will be taken if gaps are identified
The number of data security and protection incidents are measured.	In accordance with the Data Security & Reporting Incident Procedure	IG Team / IG Steering Group	On-going / monthly	IG Steering Group	An action plan will be developed by the IG Team who will present this to the IG Steering Group for approval. This will be monitored and will be closed only when all recommendations have been implemented.
IG mandatory training reports are monitored	Reports produced from on-line training system and other IG	All Line Managers / IG Team	Monthly	IG Steering Group	

	training materials.				
Awareness of compliance with key IG requirements	IG Checklists	Ward and Departmental managers / IG Team	Twice yearly	IG Team – summary results reported to IG Steering Group	
Caldicott Issues	Reported to the Caldicott Guardian	All employees	On-going	IG Steering Group	

9) Supporting documents

The following is a list of other policies, procedural documents, or guidance documents (internal or external) which employees should refer to for further details:

Ref No.	Document title	Link to document location
1	The Common Law Duty of Confidence	https://www.health-ni.gov.uk
2	The Caldicott Principles	https://www.igt.hscic.gov.uk
3	Data Protection Act 2018	https://www.gov.uk
4	UK General Data Protection Regulation	https://www.gov.uk
5	Freedom of Information Act 2000	https://www.legislation.gov.uk
6	Human Rights Act 1998	https://www.legislation.gov.uk
7	Data Protection Policy	T: Trust-wide documents
8	Environmental Information Regulations 2017	http://www.legislation.gov.uk
9	Freedom of Information Requests Procedure	T: Trust-wide documents
10	Data Security & Protection Incident Reporting Procedure	T: Trust-wide documents
11	Clinical Record Keeping Policy	T: Trust-wide documents
12	Records Management Code of Practice 2021	https://digital.nhs.uk
13	Retention of Records Policy	T: Trust-wide documents
14	Data Security & Protection Toolkit	https://www.dsptoolkit.nhs.uk/

15	Data Security & Protection Policy	T: Trust-wide documents
16	Trust Incident Reporting System	http://intranet/
17	Mental Capacity Act 2005 Policy & Procedures	T: Trust-wide documents
18	Terrorism Act 2000	https://www.legislation.gov.uk
19	Proceeds of Crime Act 2002	https://www.legislation.gov.uk
20	Working Together to Safeguard Children 2018	https://www.gov.uk
21	Information Sharing Advice for Practitioners Providing Safeguarding Services	https://www.gov.uk
22	Health and Social Care Act 2008	https://www.legislation.gov.uk
23	Nursing and Midwifery Order 2001	https://www.legislation.gov.uk
24	Medical Act 1983	https://www.legislation.gov.uk
25	Ombudsmen Health Service Commissions Act 1993	https://www.legislation.gov.uk
26	Health and Social Care Act 2012	https://www.legislation.gov.uk
27	Health Records Subject Access Requests Procedure	T: Trust-wide documents
28	Records Management Code of Practice 2021	https://digital.nhs.uk
29	Data Quality Policy	T: Trust-wide documents
30	NHS Mail Acceptable Use Policy	https://portal.nhs.net
31	EU (Withdrawal) Act	https://www.legislation.gov.uk

Appendix A – Equality Impact Assessment

At this stage, the following questions need to be considered:			
1	What is the name of the policy, strategy or project?		
2.	Briefly describe the aim of the policy, strategy, project. What needs or duty is it designed to meet?		
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any of the nine protected characteristics (as per Appendix A)?	**No**	**No**
4.	Is there evidence or other reason to believe that anyone with one or more of the nine protected characteristics have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?	**No**	**No**
5.	Has prior consultation taken place with organisations or groups of persons with one or more of the nine protected characteristics of which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?	**No**	**No**

Signed by the manager undertaking the assessment	Mark Arnold
Date completed	24/07/2024
Job Title	Head of Information Governance and Data Protection Officer

On completion of Stage 1: A full impact assessment will normally be required if you have answered YES to one or more of questions 3, 4 and 5 above.

Appendix B – Lawful Bases for Processing and rights of the Data Subject

Lawful Basis	Requirements	Rights of Data Subjects
Consent	The data subject must have given clear permission for their personal data to be disclosed for a specific purpose. This must be an opt-in process.	There is no right to object; instead, the data subject can withdraw consent at any time. Data subjects have a right to request erasure. The Trust would be required to delete information collected for that specific purpose and to inform any third party to take the same action. Any information already held would be subject to whichever lawful basis applied at the time of collection.
Contract	The processing must be necessary for the exercise of a contract that is in place with the individual, or because they have asked the data controller to take specific steps before entering into a contract.	There is no right to object to processing data that is needed for the exercise of the contract. Data subjects have a right to erasure when the data is no longer necessary. This will be subject to certain retention periods e.g. employment contracts must be kept for 6 years after the end of employment.
Legal obligation	The processing must be necessary to comply with the law, e.g. to comply with a Court Order, provide information to the Ombudsmen, or assist a regulator or inspector, such as the GMC or the CQC.	There is no right to object to processing if it is for a legal obligation. There is no right to erasure if the data is used to comply with a legal obligation or for the establishment, exercise or defence of legal claims.
Vital interests	The processing must be necessary to protect someone's life. This must only be used when it is not possible to ask for consent. This basis cannot be used for direct healthcare purposes. Safeguarding will likely fall under this lawful basis.	There is no right to object to processing of data if it is needed to protect or save a life. The data subject has a right to request erasure. This is similar to when consent is withdrawn, any information held already before vital interests processing began, would be subject to the lawful basis that applied to that data.

Lawful Basis	Requirements	Rights of Data Subjects
Public task	The processing must be necessary to perform a task in the public interest or for the Trust's official functions. As a public authority, direct healthcare services that the Trust provides will fall under this lawful basis.	The data subject has a right to object to processing. However, this is not an absolute right, and processing can continue if there are legitimate grounds, which override the interests of the individual. The individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their situation. The provision of healthcare is a public task carried out in the public interest, so if the Caldicott Principles are followed (justified purpose, minimum data, strict need-to-know, etc.), it is unlikely that an objection would require the Trust to cease processing data. An objection may be upheld if the Trust is using excessive data or sharing it unreasonably. A patient can object to their data being used for secondary purposes such as planning. There is no right to erasure of information necessary for healthcare purposes in the public interest (including provision of preventative or occupational medicine, protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices).
Legitimate interests	The processing must be necessary for the Trust's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data. This cannot apply to healthcare services or activities of the Trust.	Data subjects have a right to object to processing and a right to erasure. These would apply providing that there is no overriding legitimate interest to continue the processing.

Appendix C – Valid Consent (Patient)

The UK GDPR (Ref 4) reinforces what constitute appropriate consent procedures. Though most examples through this policy will be related to the use of information, the same principles apply to other types of consent, such as consent for treatment. From May 2018, to be valid, consent from the data subject (usually the patient) must be:

Informed – the data subject must be told how their information will be used and who the data controller is;

Able to understand – the data subject must have sufficient understanding of the implications. The age of consent is 18 years old. However, if a child is competent then it is appropriate to let the child act on their own behalf;

Able to choose – the data subject must have been given a choice and not forced to consent. There must be an active opt-in process;

Able to withdraw consent – the data subject must be given a chance to opt out at a later stage or to withdraw their consent; and

Able to communicate their decision – the data subject must be given a chance to communicate their decision or objection, in whatever way they can. A physical disability will not affect an individual's ability to understand and to consent.

If a patient does not have the capacity to give consent, or to communicate a decision, someone who has been appointed to act on their behalf must be contacted. If a child is not competent, an individual with parental responsibility should act on their behalf. If an adult is not competent, this will be someone acting as an Attorney with a registered Lasting Power of Attorney (LPA) or as a Deputy through the Court of Protection.

A search of the register of LPAs can be made at: https://www.gov.uk/government, completed forms are sent here: customerservices@publicguardian.gsi.gov.uk. However, as this may take time, if this confirmation is needed urgently, the Attorney should be asked for proof that the LPA has been registered.

Deputies are appointed by the Court of Protection when someone lacks mental capacity. During times when the data subject is 'lucid', they must remain as the decision maker. When they are lacking capacity, a Personal Welfare Deputy can act on their behalf. A Property and Financial Affairs Deputy cannot make healthcare decisions.

Where a named representative is identified their contact details should be recorded on the patient's electronic and paper records. All queries from friends or relatives should then be directed to the named representative to answer.

In the absence of a valid representative, the healthcare professional must instead make decisions. This needs to consider the patient's best interests and any previously expressed wishes and be informed by the views of relatives or carers as to the likely wishes of the patient. In this case, it may be necessary to share personal information with a patient's relatives, friends or carers to enable assessment of the patient's best interests. This does not mean they have a general right of access to the patient's health records.

For further information about patients' capacity to give consent, please refer to the Mental Capacity Act 2005 Policy and Procedures (Ref 17).

Appendix D – Examples of Disclosures

To determine whether information can be disclosed (released or shared), the legal basis must be determined, and consideration given as to whether there is any overriding confidentiality owed to the data subject.

For all types of disclosures, whether listed in this section or otherwise, the following rules must be followed.

1. Everyone has a basic right to confidentiality. This applies equally to persons living or deceased, adult or child, mentally competent or lacking capacity;
2. There must be a lawful basis for processing data within the DPA/GDPR; and
3. The rights of the data subject must be considered, e.g. have they objected to processing?
4. When considering the amount of data that can be used, remember:
5. Identifiable data should only be disclosed if absolutely necessary;
6. Minimal data must be used (consider whether personal data can be anonymised or pseudonymised); and
7. Determine who needs the information and keep it on a strict-need-to-know basis.

Disclosing Information to the Patient's Family or Friends

Information can only be shared with a patient's next of kin, friends or relatives where consent has been obtained from the patient. Next of kin do not have an automatic right to any patient information.

Where the patient is unconscious or is not competent to consent, the healthcare team may have to decide whether to release the information. This decision can be undertaken in consultation with the Trust's Caldicott Guardian or the Information Governance team.

As part of the admission process, patients may be asked in advance whether they wish for information about their care to be shared with a named representative (usually a relative or friend).

Disclosing Information to the Police, Fraud Officer or Other Enforcement Agency

All enquiries from enforcement agencies should be referred to a senior/nurse manager, or the on-call Manager. The police or other enforcement agencies do not have an automatic right to information. No information should be given without the data subject's consent, unless one of the exemptions under the DPA 2018 applies, such as when:

- It is necessary for the prevention or detection of an unlawful act (crime). It must be unreasonable to gain consent and sharing must be for reasons of substantial public interest. Examples of this could be a serious assault, attempted murder or sexual assault, including but not limited to, where a girl under the age of 18 has been subject to genital mutilation as per the Female Genital Mutilation Act (2003).
- It is necessary to protect the public against dishonesty. It must be unreasonable to gain consent and sharing must be for reasons of substantial public interest. Examples of this could be dishonesty relating to a clinician's qualifications, malpractice, fitness to practice concerns or serious failures/mismanagement of a healthcare body.
- It is necessary to protect the public against unlawful acts and dishonesty (regulatory). It must be unreasonable to gain consent and sharing must be for reasons of substantial public interest. Examples of this include a failure to act on a requirement imposed by legislation or accepted principles of good practice.

- It is necessary to prevent fraud. The disclosure must be to a member of an anti-fraud organisation.
- It is necessary due to a suspicion of terrorist financing or money laundering. Disclosures can be made pursuant to the Terrorism Act 2000 (Ref 18) or the Proceeds of Crime Act 2002 (Ref 19), respectively.

In general requests for information from the police, fraud officer or other enforcement agency will be made in writing (the police have a standard form for this purpose) and will be signed by the data subject to confirm that they give their consent to disclosure of their personal information.

In addition to the areas above where information can be disclosed to the police or other enforcement agencies, Article 23 (d) of the UK GDPR states that the data subject cannot object to or restrict the processing of data if it relates to 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

If information sharing is essential at the time of a major incident, for example, please refer to the checklist "Disclosure of personal information_urgent requests" which is held in the iRespond system managed by the Resilience Team and available on staff desktops.

Disclosing Information for Safeguarding Concerns

The DPA 2018 allows for processing of special category data when there is risk to an individual of harm or for their wellbeing. This includes a risk of neglect or physical, mental or emotional harm; or, to physical, mental or emotional wellbeing.

Consent should be sought where possible and the wishes of the child or vulnerable adult should also be taken into account. However, disclosure of information is permitted when it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child or vulnerable adult at risk.

For more information please refer to Working Together to Safeguarding Children 2018 (Ref 20) and the Information Sharing Advice for Practitioners Providing Safeguarding Services (Ref 21).

Disclosing Information to Regulators and the Ombudsmen

The Care Quality Commission (CQC) has powers under the Health and Social Care Act 2008 (Ref 22) to access medical records for the purposes of exercising its functions. Inspectors will only use this power to look at a patient's medical records where there is a defined reason to do so, and where intrusion to the privacy of that patient is justified and proportionate. The national data opt-out will not apply to CQC's access to records. The CQC will respect the patient's wishes unless there is an overriding need to look at that record.

The UK healthcare regulators have a statutory right to information when conducting investigations, known as fitness to practise cases. The two largest of these regulators, the Nursing and Midwifery Council (NMC) and the General Medical Council (GMC) have this power pursuant to the Nursing & Midwifery Order 2001 section 25.1 (Ref 23) and the Medical Act 1983 (Amendment) Order 2000 Article 4 (Ref 24), respectively.

The Parliamentary and Health Service Ombudsman (PHSO) is an independent complaint handling service. Information related to an unresolved complaint can be shared with the Ombudsman pursuant to the Ombudsmen Health Service Commissioners Act 1993 section 12 (Ref 25).

Disclosing Information for Commissioning Purposes

Integrated Care Boards (ICBs) are not permitted to process personally identifiable data for general commissioning purposes without authorisation from the data subject. The ICB can sometimes collate identifiable information between primary and/or acute care for support services or further analysis provided by external processors; this is always under a sharing/processing agreement. Any data used/stored by the ICB for secondary uses must be anonymised. Under the Health and Social Care Act 2012 (Ref 26), NHS Digital provides an intermediary service called Data Services for Commissioners Regional Office (DSCRO). For general funding or commissioning requests, the patient level data must be sent to the DSCRO directly, who will link a patient's events without revealing the identity of that person. For requests relating to complaints, these should be done with the consent of the data subject. Request a copy of the consent before any data is shared.

Disclosing Information for Auditing Purposes

As a public authority, the Trust is required to publish its annual report and accounts. There is also an internal and external audit assurance and risk programme. To facilitate these processes, the auditor(s) will need access to confidential information, often of a sensitive financial nature or in relation to risk management.

The auditor(s) will work under the terms of a contract and their industry code of ethics, as well as agreeing with the Trust the terms of reference for the audit. Information requested by the auditor can include, but is not limited to, sets of accounts, risk registers and minutes of meetings. These can be provided under the public task lawful basis as there is a requirement to ensure that the Trust operates correctly and efficiently as a public authority. No patient identifiable data should ever be disclosed.

Disclosing Information to the Media

Requests for information by the media must be dealt with by authorised Senior Managers and/or the Trust Communications team on 01793 60(4418). If a request is received from the media in person or by phone, they must be referred to the On-Call Manager or to the Trust Communications team.

Disclosing Information to Third Party and Partner Organisations

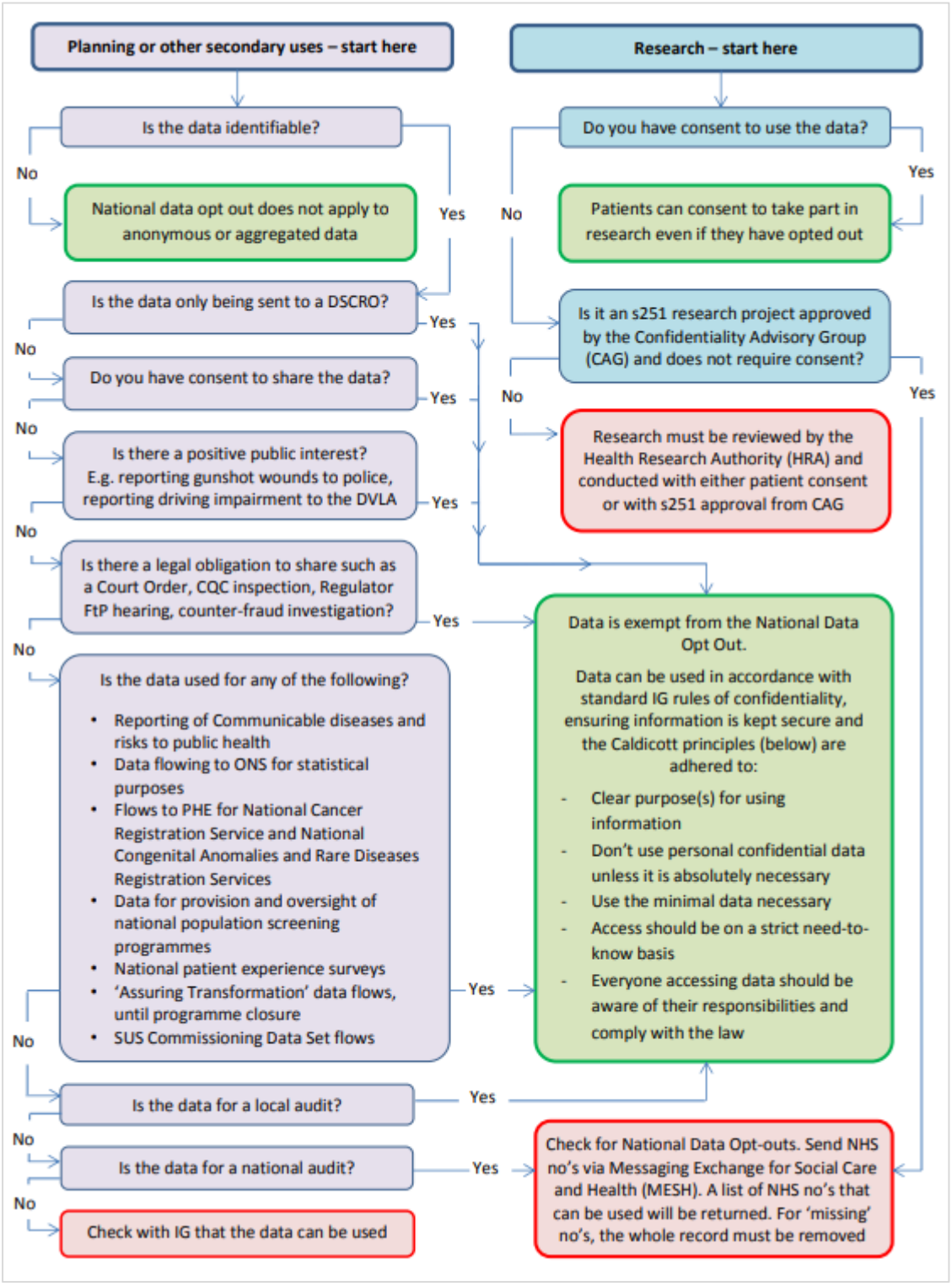
Where another person/NHS organisation requests information about a patient, the requestor must be able to verify their identity and provide evidence that they have a lawful basis to receive the information. This includes requests from GPs, other hospitals, social services, etc. If the requestor's identity cannot be verified and a lawful basis for sharing is not identified, then no information must be released.

Subject Access Requests (SARs) and Freedom of Information (FOI) Requests

For SARs please refer to the Health Records Subject Access Requests Procedure (Ref 27) and for FOI requests please refer to the Freedom of Information Requests Procedure (Ref 9).

Appendix E – National Data Opt-Out Flowchart

Use the flowchart below to determine whether the national data opt-out applies. If it does then information about people who have opted out must be removed from datasets. To do this, follow the local process to check NHS numbers. Speak to the IG team for more details.



Appendix F – Offences in Relation to Personal Data

This is a list of offences under the various data protection legislation, NHS Codes of practice (including Regulator's Codes of Practice) and common law. This list is not exhaustive.

It is an offence for a person knowingly or recklessly—

- to access, obtain and/or disclose personal data without the consent of the controller or for a valid business need under a separate lawful basis;
- alter or amend information, and/or add information to a record, with the intention of making an incorrect or inaccurate record;
- delete personal data which has not met the retention period set out in Trust policy and which has not been reviewed and agreed for destruction. This includes any data which has been made redundant or incomprehensible through defacing, altering or damaging the data;
- to make data unavailable – temporarily or permanently – through their own actions, or through the actions of other parties (such as threat actors);
- to destroy, delete, conceal and/or make unavailable – temporarily or permanently – any data which has been requested under a Subject Access Request, Freedom of Information Act request, Court Order, Inquiry or any other formal request process;
- to sell personal data. It is also an offence to advertise or indicate that personal data is or may be for sale, or to offer to access, obtain and/or disclose personal data, regardless of whether there is any monetary value placed on this action;
- after obtaining personal data, to retain it without the consent of the controller or for a valid business need under a separate lawful basis;
- use another member of staff's credentials, login details and/or smartcard access in order to access, obtain and/or disclose personal data;
- to re-identify information that is de-identified personal data, without the consent of the controller or for a valid business need under a separate lawful basis;
- to process personal data that is information that has been re-identified, without the consent of the controller or for a valid business need under a separate lawful basis.

Offences under the Computer Misuse Act 1990

The Act contains three criminal offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

The Computer Misuse Act has also made it an offence to make, adapt, supply or offer to supply any article which is 'likely to be used to commit, or to assist in the commission of, a hacking or unauthorised modification offence'.

Appendix G – Code of Best Practice for Employees in Respect of Confidentiality

Introduction

People working within the National Health Service (NHS) are bound by a legal duty of confidentiality to protect personal information that they may encounter during the course of their work. In addition, healthcare and other professionals have standards of confidentiality within their own professions' Code of Conduct.

All employees are responsible for maintaining the confidentiality of information gained during their period of work for the Trust, and that responsibility continues after employees cease working for the Trust.

> **Confidential information** - is defined as any information that would be expected to be used in confidence. Generally, it is split into person-identifiable data (PID) which is anything that contains the means to identify a person, e.g. name, date of birth, address, postcode, NHS number, and special categories of data, such as physical or mental health/condition, race, ethnic origin, religion, sex life or sexual orientation.

Ensuring Data Subjects are Aware of what Happens to their Information

Most of the personal information that the Trust holds and manages is related to either patients or employees. Employees who encounter patients and other employees, e.g. those in Human Resources, Payroll etc., must be able to direct them to relevant guidance about what happens to their information. This can be by:

- Ensuring that privacy notices, information leaflets etc., have been given to, read and understood by the data subject;
- Providing advice about when information is to be recorded or when records are being accessed or disclosed, including who is to record/access information, and to whom they will be disclosing information. The Trust's privacy notices for patients and staff are available via the internet and the intranet.
- Ensuring that data subjects are aware of choices about how their information may be disclosed, ensuring that they have no concerns or queries;
- Recording the preferences for sharing information such as with friends or family or if applicable, who the patient's representative is;
- Answering queries or, where necessary, directing the person to others who can assist. More detailed or technical questions regarding the Trust's use of information, may be referred to the Information Governance team via gwh.info.gov@nhs.net;
- Respecting the data subject's rights, including the right to have access to their records and the right to object to processing;
- Asking before using personal information in ways that do not directly contribute to or support the delivery of their care, or as part of their employment contract with the Trust;
- Respecting the data subject's to restrict the disclosure or use of information, except where exceptional circumstances apply; and
- Treating children equally with the same rights as adults if they can understand the consequences and risks of any decision made.

Leaflets to assist patients and employees are available from the Information Governance team via: gwh.info.gov@nhs.net. Information about confidentiality is included in the standard induction and refresher training for all employees.

Records Management / Data Quality

The Trust complies with the 12 generic record keeping standards approved by the Academy of Medical Royal Colleges. These are listed in the Trust's Clinical Record Keeping Policy.

Retention periods for all types of records are listed in the Records Management Code of Practice for Health & Social Care 2016 (Ref 28). This list is also available on the Trust intranet. Further information about records retention and disposal may be found in the Trust's Retention of Records Policy (Ref 13).

All employees are personally responsible for the quality of data entered by themselves, or on their behalf, on the Trust's computerised systems. Whether held on paper or electronically, employees have a responsibility to ensure that the data is accurate, timely, and as complete as possible.

This responsibility is clarified in the employee's job description and by their professional body such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC), Health and Care Professions Council etc. (and monitored via ongoing supervision/appraisal). It is essential that any alterations or updated information is amended as soon as possible in records and on Patient Information Systems to provide up-to-date information to support the delivery of care and to meet statutory requirements, e.g. Information Governance data-quality standards. Please refer to the Trust's Data Quality Policy (Ref 29) for further information.

Storage / Access to Information

General

Employees are strictly forbidden to access confidential information held by the Trust about themselves, so if an employee requires access to their personal information, this should be done using their rights under the Data Protection Act 2018. Refer to the Trust's Data Protection Policy (Ref 7) for further information.

Employees are strictly forbidden to access personal or special category information relating to colleagues, family, friends or acquaintances, or any other person, including patients, unless they are directly involved in that patient's care, or work in an administrative role such as People Operations or Payroll and have a legitimate work-related need to access the information. If an employee becomes aware that they are involved in the care of a patient who is known to them, the employee should notify the line manager or the consultant/doctor in charge that there may be a conflict of interest.

Employees are authorised to access their own employment details contained within the self-service portal of ESR.

If an employee's conduct includes any of the actions described above or contravenes any guidance found in the healthcare regulators codes of conduct, for example the GMC Code of Confidentiality, this will be a breach of confidentiality and may result in disciplinary action.

Access to Electronic Systems

Employees are given access to electronic systems which are relevant to their role within the Trust. Access is granted with the understanding that:

- They will act in accordance with their employment contract with regards to accessing information;
- Any system specific terms and conditions of use will be followed;
- They are aware that a user's computer use and conduct can be monitored and that audit trails can be produced from Trust systems. They are aware that electronic systems will have role/position based access control (RBAC/PBAC);

- They will notify the relevant system administrator if their role changes and they no longer require access to a system;
- For externally hosted systems, sensitive or special category information must not be stored on the system unless a Data Protection Impact Assessment (DPIA) has been completed;
- Confidential information stored in electronic format must not be stored unencrypted on the local hard drives of Personal Computers (PCs) or on removable media;
- Information must be saved on the appropriate systems or network drives provided by the Trust e.g. T: drive;
- Confidential information can be held on removable media for the purposes of authorised data transfer. Memory sticks, CDs/DVDs, dictation tapes and other media must be encrypted and kept in locked storage when not in use.

Access to Shared Electronic Systems

The Trust is a joint data controller or processor for shared systems such as the National Care Records Service (NCRS) and the Integrated Care System (ICR); this list is not exhaustive. These systems are hosted, or contributed to, by numerous health or social care providers such as primary care, other secondary care sites, and the local authorities, and data can also be accessed by the Integrated Care Board (ICB). When using shared systems, all Trust staff must adhere to the applicable policies, such as this Information Governance Policy, as well as any additional licence agreements or terms and conditions of use. For the avoidance of doubt, this applies to all data held within the system, not just data contributed or used by the Trust.

Misuse of any of these systems or inappropriate or unauthorised access to any data held within these systems will result in an investigation and may involve access being revoked and/or disciplinary procedures.

Storage and Access to Physical Records/Locations

Physical records, such as paper-based health or personnel records, must be held securely and accessed only by those who have a need to know. The following measures are in place to protect physical records and to ensure their availability:

- Access to areas in the hospital which are not accessible to the general public is controlled through the use of Keri Cards;
    - Keri cards must not be given to anybody else to use; this includes both Trust staff (including volunteers, agency, bank staff, contractors, etc.) and people who do not work at the Trust such as family and friends
    - Keri cards must not be used when staff are off duty to gain access to wards and other areas
    - Where appropriate, the wearer must announce their intention to enter locked wards, etc, via the intercom provided
    - The wearer must always have their Keri card in a place which is visible, such as on a breakable lanyard which complies with health and safety regulations or clipped to clothing
- Paper based records are subject to security procedures which include:
    - Locking doors
    - Locking filing cabinets
    - Managing access with the use of keys and swipe cards

- Paper-based confidential information is stored securely when not in use. (Secure storage is particularly important at night-time and over weekends when buildings/offices may be unoccupied for a long period of time);
- If moved, physical records must be tracked to the correct location.

Sharing Information

Verifying Identity

When sharing information with individuals in person, during a virtual consultation/meeting or over the telephone it is important to confirm the individual's identity before any confidential or sensitive information is released.

To confirm the identity of the patient over the phone, during a virtual consultation/meeting or in person, a minimum of three questions must be asked before any information is disclosed. Example questions could be for the patient to confirm their date of birth, address and postcode, their treatment or dates of appointment, their hospital/NHS number.

Similarly this process must be applied to those responsible for sharing information about employees. This is particularly important as, if employees identified by name only, this may result in incorrect identification as there is often more than one employee with the same or a similar name.

When sharing information by post, email or fax, contact information should be checked for accuracy. This can be done by checking details at each appointment or by checking a second system, such as the NHS Spine, or the Electronic Staff Record (ESR).

Post / Mail

General

General postage rules may be found on the Trust's intranet site. Post which needs additional security, such as a copy of a patient's health record or bulky material, should be sent as a tracked recorded delivery. Items which include a signature and need to be sent via Royal Mail First Class, Track & Trace or Signed For services must be authorised by a Divisional Director or equivalent. A tracking number should be supplied with this delivery which can be shared with the recipient so they know where the post currently is and when it can be expected. A signature is also required when the post is delivered.

Couriers can also be used when sending post which requires additional security. Couriers must be part of the Crown Commercial Services approved supplier list which can be found here: http://ccs-agreements.cabinetoffice.gov.uk/suppliers.

Content

- Items sent in the post can be letters, samples, discs or CDs, portable devices such as USB sticks, images such as clinical photography or x-rays, video recordings or anything else which is sent through the postal system;
- Due to the varying information and volume of post which is sent, all mail must be checked before it is placed into an envelope or package;
- Checks are to ensure that all information is adequate, relevant and not excessive. All information should relate to the subject of the letter and should not include anything additional or relating to a third party. Before sealing the envelope or package, it is important to check that no extra documents or information about third parties has been included by mistake.

Address

- There is a facility to print address labels from some clinical systems. Before address labels are printed, the details must be checked to ensure that the correct information is being printed.

- When handwriting addresses on envelopes, the address should be checked for accuracy. This should be copied from an up-to-date system or recent entry in the physical notes.
- Whether the address has been printed or handwritten, the address must be checked to ensure that the address relates to the correct person or organisation, and must be fully addressed clear, visible and legible.
- People and organisations change contact details regularly, so addresses should be double checked wherever possible against a separate record to ensure that the most up-to-date contact details are being used. If staff have access to the Integrated Care Record (ICR) it is possible to check demographics that are recorded at other providers such as the GP, which may be more up-to-date. To do this; firstly, retrieve the patient in the ICR and on the landing page, click on the arrow to expand the 'Record Content & Demographics' widget, secondly, navigate between the 'Care Providers' to see the demographics data submitted by each provider.

Envelope

- All envelopes or packages that are used to send mail must be sealed securely and the packaging or envelope must not be re-used or stuck down with tape. This is not adequate security to stop the letter being opened and there will be no way to know whether the letter has been tampered with.
- Envelopes or packages should be opaque so that the contents are not visible other than a recipient's name and address.
- All mail which contains personal or sensitive data must have the words 'Private and confidential' clearly visible on the front of the envelope or package.
- Internal post containing person-identifiable or other confidential data must only be sent in a securely sealed, correctly addressed envelope. Only envelopes that are designed to be re-used, e.g. have multiple address boxes, can be re-used, and the envelope must not be torn or the integrity compromised. Single use envelopes must not be re-used, as there is a risk that they will go astray.

Phone

General

- Data subjects have the right to privacy so Trust staff must not talk to them or discuss their personal details over the phone in a public area where the conversation may be overheard.
- Unless there is justified reason to speak to someone on a patient's behalf, e.g. they have given their consent or it is in their best interests, contact should be with the patient directly.
- Avoid "alarmist" language such as 'it's confidential' or jargon like 'fast track'.
- If you think you may need to contact the patient by phone, ask if you can call them at work, at home or on a mobile.
- Ask if you can leave messages.
- Before contacting staff in other areas of the Trust or those in external agencies always ensure you have a lawful basis to process their information.

Making Calls

- Always confirm who you are speaking to before releasing information.
- Document actions taken - Healthcare professionals and carers may need this information to provide best care for the patient, and you may need to provide it without consent in circumstances that warrant it.

- When calling someone at the request of the patient, or because they need to be contacted, always check who answers the phone if possible.

Leaving messages on Answerphones:

Double check it is the correct number. Unless you can guarantee that the message will be delivered to and received by the correct patient then do not leave a message. Patient confidentiality can be breached from messages left on answer phones or voicemail, resulting in embarrassing or harmful situations arising.

If you must 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 mention the Trust or leave any clinical information.

When the phone is answered by someone other than the patient, always ask to speak to the patient, but don't say where you are calling from. 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 if the organisation name does not imply anything to do with the health of the patient.

If the patient is not present, then unless there is a degree of urgency do not leave a message but ask about a suitable time to call back.

If the patient is present but unable to speak (either due to language or physical difficulties), ask to speak to their 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).

Receiving Calls

Personal information relating to outpatients must only be released to the patient themselves. For inpatients, calls should be directed to the ward/department where the patient is located, except where the ward location/department would reveal information about the patient when answered; for example, the delivery suite or birthing centre, cancer services, sexual health. Where the patient is conscious and considered competent, patient consent should always be obtained before information about them is released. If consent cannot be obtained immediately, take a message from the friend or relative and inform the patient of the call when appropriate.

If someone has called you and you are not sure who they are, if possible, ring them back through a switchboard or number that we have recorded. A caller's identity can be confirmed by calling them back on an independently verified contact number (e.g. a number available on their website). 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. Get the caller to tell you things about the patient, 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.

Unless you have patient consent, or can justify why the caller should know, then very limited information can be provided. Check the patient records to see if someone is acting on behalf of a patient who can't call for themselves. Without the above checks being made, confidential information cannot be disclosed. If in doubt about answering enquiries, employees should check with the consultant/doctor in charge of the patient's care or with a line manager.

Text Messages

The Trust uses various systems to text either patients or staff. Texts can only be used in certain circumstances; otherwise it will be a breach of the Privacy and Electronic Communications Regulations. The ICO and NHS England have clarified that the following uses of text messages will not be considered marketing, and are therefore, acceptable in moderation:

- appointment reminder or confirmation messages;
- acknowledgment messages such as confirming receipt of information or applications;
- test result messages; and
- messages about changes to services.

Email

General

The Trust uses NHSMail as its email system which means that all emails between NHS mail accounts are secure. Also, emails sent from an NHSMail email account (@nhs.net) to other email addresses which are government domains will be encrypted and secure.

Content of an email

When sending an email, check to make sure that the content and any attachments to the email are accurate and that it is only meant for that recipient. If sending an email to multiple recipients, check that any personal or sensitive data included has been consented to be shared or is subject to a justified reason to share. Any data which does not have a justified reason to share must be removed. Also, check that all addresses in an email if selecting 'reply all' to ensure they are secure addresses.

If an email is to be sent to anyone outside of the Trust who is not on the NHSmail system (has an email address ending in @nhs.net), it is recommended that no patient and/or staff identifiers are used in the subject line of the email.

Replying to a patient's email

Corresponding with patients by email must only be done in very limited circumstances. The following guidance must be adhered to:

- Obtain the patient's full written consent
- Make sure the patient understands the risks (see below)
- File a copy of this consent in the patient's health record
- Use the minimum amount of information possible
- Confirm the identity of the requestor first
- Use [secure] in the subject line (see Sending a Secure Email section below)

Patients are to be advised that any information transferred out of the Trust's network is not secure and could be intercepted by others who have access to the email account. Their personal information could be open to access by malicious or criminal cyber products that can intercept emails without authority. The Trust cannot be held responsible for the security of the patient's personal information coming into and going out of its network.

Patients must also be advised that it is their responsibility to inform the Trust if their email address changes.

It is recognised that the Trust is moving forward with using email to send appointment letters and reminders to patients. Any department or team etc. that is considering using email as their preferred method of communicating information with patients must advised the Information Governance team in order that risk assessments can be made and a process set up to be followed by the department or team.

Auto forwarding/supplying alternative address

Auto forwarding is not used in this Trust, however, as part of an out of office response you can direct people to send email messages to an alternative business email address.

The NHSMail system is to be used solely for work-related activities, in accordance with the NHSMail Acceptable Use Policy (Ref 30)

It is strictly prohibited to use personal email addresses (@gmail.com, @hotmail.com, @doctors.org.uk, etc.) for Trust business as they are insecure. As such these must not be placed in out of office responses or to set up auto-forwarding to these accounts.

Allowing someone else access to your emails

To allow another member of staff to access your emails you must set up appropriate delegate permissions. Employees must never share their usernames and passwords with anyone. For assistance with configuring delegate access, please contact the IT Service Desk.

Sending a 'Secure' Email

NHSmail provides an option to encrypt the email to organisations or people outside of the NHSmail network. Some users may have this on their Outlook client. If not, to do this use [secure] as the first words in the subject line, for example:

To: gwh.info.gov@nhs.net

Subject: [secure] Staff audit report

Note, this should only be used to enhance security and should not be relied on as the only method to protect information. See the NHS Digital guidance for more information: https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email.

Sending Large Files

Egress, the NHSmail supplier, has produced a large file transfer system for NHSmail. Some users may have this option on their Outlook client. If not, then go to: https://lft.nhs.net. The Egress login details are the same as your NHSmail credentials.

This service will require the recipient to create an account with Egress once they have received the email informing them that the large file(s) are available to download.

Video Consultations

Arranging Calls

A video consultation with a patient, must be carried out using one of the approved systems in place at the Trust. When arranging a video consultation, a new link must be used for every meeting. If links are re-used then this increases the risk of the meetings being attended/interrupted by unintended guests. This is especially important if meeting links are sent to multiple recipients.

Location

The video consultation must be held in a private location to the same standards as a face-to-face appointment. The room must be private, the door must be closed and there must be no other people in the room, unless they are part of the team that are conducting the call. The room must allow for privacy of conversations and staff must be aware of who may be able to overhear conversations, as per face-to-face consultations. If the conversation can be overheard, then that location must not be used. In addition, it is advisable that notes are available during the consultation in either electronic or hard-copy format; therefore, the location must be secure so that these notes cannot be seen, stolen, viewed, or accessed by anyone else.

Conducting the Call

During the call, the clinician must act as if the consultation was face-to-face. This means that there must be a positive identity check of the patient and there must be an adequate way to conduct the consultation remotely. If the consultation cannot provide the right level of assurance, for example, because the patient cannot be examined efficiently, or because the patient has someone else with them and there is a safeguarding concern, then the appointment must be rearranged as a face-to-face consultation.

There is guidance on the IG intranet pages on how to conduct video consultations.

Collaboration Tools

The Trust supports the use of online collaboration tools to improve efficient working between teams that are working remotely, or between external organisations. However, to use these tools the following steps must be taken:

- Check if there are any Trust-approved tools which can provide the service you need (the Trust publishes approved DPIAs on the website) or you can contact the IG team for further information
- If a new tool is being used, then a DPIA must be completed
- Liaise with both the IG and IT teams to determine whether there is any risk to data or technical specifications that need to be implemented
- Agree to any terms and conditions of use, if applicable

N365

MS Teams

General

Be aware of your surroundings; and pay attention to what can be seen behind you. If you are working from home, move to a private location where the screen cannot be seen or the conversation overheard. Whether you are within the Trust, or working remotely, use backgrounds within Teams, such as the Trust-approved backgrounds available on the Intranet to download. In addition, wherever possible but within reason, use a headset to keep discussions confidential, take calls in a separate room with the door closed and close exterior doors or windows.

Teams and Channels can be created for organisations by NHS Mail Local Administrators. These are useful to work collaboratively and to share documentation or support discussions between the relevant parties. Only users with an nhs.net or other NHS accredited email account can be added to a team. The Team admin user should restrict membership to each channel to protect any sensitive information which should not be shared with a wider membership. The Teams Channels should never be used as the primary storage location as data held in MS Teams is not backed-up or recoverable.

Meetings

Do not reuse Teams links due to the chat and files being continuously available. There is also a risk that any guests or one-off invitees to a recurring meeting (even if they only join once) will have full access to the chat during that meeting and afterwards. You should always set up non-reccurring meeting invites if guests are invited. Use the waiting room function for external guests to a meeting and be aware they will have access to chat for all meetings for that discussion.

It is possible to record a meeting on Teams. If you intend to record meetings, please inform the other participants so that they can turn their camera off if they do not wish to be viewed. Recordings should be on a case-by-case basis and not done routinely. If there are on-going reasons for recording meetings, such as to help take accurate minutes, then there must be a process to delete the recording

once the minutes have been agreed as accurate. This is for confidentiality reasons and due to storage limits on the Trust network.

Chats

Any message you send via a chat is retained on Teams and will be considered a record. Therefore, it is subject to both Subject Access Requests and Freedom of Information requests.

You should not use inappropriate language or share unauthorised content. The same behavioural standards should be adhered to as for sending emails. Any record / chat / discussion pertaining to a patient must be saved to the patient record and not stored on Teams. Chats on Teams can be searched by clicking on 'Chat' and entering a search term in the search bar at the top of the screen. Teams is a corporate system and any communication, including 1-to-1 conversations, should be restricted to business-related discussion. Personal discussion should not take place over any corporate service.

Discussions about other members of staff are subject to the Data Protection Act 2018 and an individual's right of access to information held about them. Some Team chats are viewable by several users. You should always ensure what you are discussing is appropriate for the people who have access.

Files

Teams is a collaboration workspace, and not a records management system. You should continue to save important documents in the network drive locations already in place. You may work collaboratively on draft versions of documents on Teams, or share project documents but the final version must be saved to the appropriate location on the shared drive as per normal practice. Each discussion should appoint a role whose responsibility it is to save documents to drives to avoid confusion about who is undertaking this. When using Teams remotely on non-NHS equipment, work files must not be synced or saved to your own equipment. Save files to your work network locations only.

OneDrive

OneDrive was originally created as a cloud back-up storage facility. This mean that files could be synced from a computer hard drive to the cloud, ensuring that if something went wrong then the file could be restored. As it was stored in the cloud, it could also be accessed from other locations.

Due to the flexibility of access, OneDrive is being used increasingly as a collaboration site where documents can be shared with others, worked on collaboratively and accessed from remote locations. If using OneDrive as a file sharing tool or way of remotely accessing documents, you must follow these rules:

- General sharing/access: Files are set to private as default. If you want to share information always check who you are giving access to. If you can limit the access to single documents this is better. If access to folders is given then all files within that folder will become visible. If you have given access to information, this must be reviewed regularly and access removed when no longer required. In addition, the standard IG rules will apply and confidential data must not be shared unless it is absolutely necessary, it is not excessive, there is a need-to-know and there is a clear lawful basis.
- Back-ups: Files that are worked on in OneDrive, including files that are being co-edited are saved as you work. HOWEVER, OneDrive's purpose was to provide a back-up to hard drives. This means that data must be saved on the Trust network. There is no back-up of the OneDrive – this is not the responsibility of the Trust IT department. If a document or folder is deleted by mistake or becomes corrupt then you can check the OneDrive recycle bin but if the file is not there, it cannot be recovered.

- Storage and retention: As above, all files and folders must be saved to the Trust network. The original or only version of patient data or decision-making documentation which may have a legal impact should not be saved on OneDrive ,. When documentation that is under development or review is no longer needed on OneDrive, then it must be deleted at the earliest opportunity and deleted from the recycle bin.
- Leavers: OneDrive access is provided by the Trust and is a tool to support staff when working. No data should be saved on the OneDrive which has not been saved on the Trust network. If you leave the Trust then access to OneDrive will be removed and data will be set to delete automatically. Your manager will be granted access to the drive for 30 days to ensure that no Trust data is lost. If you are moving to another NHS healthcare organisation and you have copies of information which may be helpful to you, such as a copy of a policy, then this can be taken with you. However, no files or folders which contain confidential data, can be taken unless approval has been sought from the Trust's Information Governance team.

Physical Transfer of Records

Employees must always give the highest priority to the security of records they are transporting, especially in the case of records containing personal, sensitive or confidential information. All sensitive personal information must be:

- Transported in a suitable lockable or sealed container or folder, and in an encrypted format where held electronically;
- Recorded in the relevant departmental tracking system by the person transporting the records;
- Kept away from anyone who is eating, drinking or smoking near records, or transported in a vehicle which does not contain hazardous materials or liquids which could spill and damage them;
- Supervised and enclosed in a suitable container (e.g. an envelope or covered trolley), to prevent unauthorised access whilst in transit on-site;
- Handled carefully when being loaded, transported or unloaded;
- Packed carefully into vehicles to ensure that they will not be damaged by the movement of the vehicle; and
- Transported in fully enclosed vehicles so that they are protected from exposure to the weather, excessive light and other risks such as theft. Where regular transfers of information are made with partner organisations, minimum datasets should be agreed by both parties to ensure that only information necessary for the task in hand is shared.

Employees must be authorised to take the information off-site – it is normally the line manager who grants this authorisation and must ensure that only the minimum of information is taken off-site.

For paper-based medical records, details of the records and the employee must be entered on the case note tracking system, and the Health Records Manager must be informed. The records must be transported in secure sealed bags.

For other paper-based files/records, a log must be kept on-site of which records have been taken, when and by whom, where they are being taken, and when they are to be returned.

For electronic files/records, the information must be held in encrypted form on a CD/DVD, memory stick or other removable device/media. There may be exceptional situations where it is necessary for person-identifiable information to be stored on the encrypted hard drive of a laptop, but it is best practice to avoid doing so if at all possible. Person-identifiable information must never be held on the unencrypted hard drive of any PC.

Whilst the information/records are off-site, the employee has personal responsibility to ensure that the information is kept secure and confidential. This means that the employee must not make any

copies or allow any copies to be made, and must not allow friends, colleagues or other family members to see any of the information, including any details printed on the outside of paper folders.

When files/records are returned to the workplace, they must be transported in secure containers or in sealed packages. When paper records have been returned to the Trust's premises, their return must be logged. Electronic files/records on removable devices/media must be virus-checked before being loaded onto any of the Trust's systems or network drives.

Faxing

Faxes are no longer used within the NHS. Any confidential information held by the organisation should only be sent by fax where it is necessary and other means of transfer are not available, for example, during a cyber-attack where the email system is not available.

Disclosing / Sharing Information

The disclosure or sharing of confidential information must only be on a 'need to know' basis and to an individual that has a legitimate right to receive it. Anonymised information rather than person-identifiable information must be used wherever possible, and any use of person-identifiable information must have a legal basis or be for justified purposes.

Security of Information

All confidential information must be treated in the strictest confidence and must always be held securely. It must be retained safely for as long as necessary and destroyed securely when no longer required. Employees can help to keep information secure by following these simple rules:

- Any confidential information, held in any format, which is received from or sent to another individual, must be secure in transit and addressed correctly;
- Do not talk about patients or employees in public areas or where there is a risk of being overheard;
- Do not breach confidentiality or post inappropriate comments on social networking sites. Even if personal details are not disclosed they could still be deduced
- Confidential information must not be stored on the unencrypted hard drive of any computer which is provided by the Trust or is used by the employee for work purposes;
- Confidential information must be encrypted when stored electronically on any mobile or removable device/media or when transmitted/transferred electronically;
- Locations where information can be accessed, e.g. health records, must be physically secure;
- Do not leave any patient records or confidential information lying around unattended;
- The security of passwords and of access codes to locked areas must be maintained;
- Computers must be logged-off or locked when left unattended;
- Do not allow any computer monitors or other displays of information to be seen by members of the public or by anyone without a right to view the information.
- Passwords issued to or created by employees must be regarded as confidential. They must not be communicated to anyone else nor should they be written down;
- Passwords should not indicate the employee involved or the system being accessed.
- Passwords should not be obvious or guessable – for example, avoid using dates of birth, family names, pet's names or sports teams which might be known to others (or targeted through phishing emails). Passwords should never be common words/phrases such as 'Password123' or 'Pa55word'. They should not be repeated where the same password is used over again. They should not be written down.
- Staff must only use Trust-approved password management software such as the Single sign-on or Imprivata

Further information about password control and format etc., is given at the relevant training session or when the user name and password are issued.

Employees must not attempt to bypass or defeat the Trust's security systems, or to obtain or use passwords or privileges issued to other employees. Any such attempts to breach security should be reported immediately to the Information Governance team via gwh.info.gov@nhs.net or via the IT Service Desk on 01793 60(5858). Attempts to breach security may be regarded as a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 2018,(Ref 3) which can lead to criminal action being taken against the individual(s) involved.

- All removable media and mobile devices, including CDs and DVDs, used by the NHS and its staff must be encrypted;
- Only encrypted USB memory sticks can be used on Trust computers to save information - if you need to use a USB memory stick you should contact the IT Service Desk.
- Although Trust encrypted USB memory sticks are secure they are still prone to corruption, loss or theft. You must therefore only ever save information to a USB memory stick temporarily and where there is a copy securely saved to a Trust network drive.
- Any new information saved to the USB memory stick must be copied back to the Trust network at the earliest opportunity.

Destruction of Information

Any paper which contains confidential data relating to staff, patients, or other individuals must be placed in the confidential waste bins. If using confidential waste bags, never leave these unattended in a corridor or other unsecure area.

If you are not sure whether the paper you have contains confidential information, always place it in the confidential waste bins to be safe. Only paper may be placed in the confidential waste bins.

If personal or confidential information is stored on electronic media (e.g. CDs, DVDs, Floppy Discs, USB Memory Sticks, etc.), please contact the IT Service Desk for advice on how to dispose of these securely.

Incident Reporting

If an incident occurs, inform your manager and/or the Information Governance Team as soon as possible. Usually on the day that the incident occurred or on the day that it became known. Report the incident on the Trust's Incident Reporting System, and, if you can do something to resolve the problem quickly, try to do this first.

If an employee feels that to report a breach or potential/suspected breach of confidentiality or security would compromise their position within the Trust, they may report it directly to the Information Governance team or in accordance with the Trust's Freedom to Speak Up Policy.

Do not ignore or cover up incidents. Investigations are not against individuals, they will look into the process that was followed which led to the breach. Remember, if incidents are not reported then improvements cannot be made.

The ICO can take action against the Trust, or if the breach was deliberate or seriously negligent, against individuals. Unreported incidents or breaches with no remedial action will be considered more serious. Deliberate or seriously negligent breaches may result in disciplinary action, a criminal prosecution and/or a fine. Individuals may also be referred to their healthcare regulator if it is deemed that their fitness to practise may be impaired or there has been a deliberate breach of their respective codes of practice, ethics or confidentiality.