St Helens and Knowsley Teaching Hospitals NHS Trust

Code of Confidentiality

This document is a guide to required practice and responsibility for those who work within or under contract to the Trust concerning confidentiality of staff and patient information and patients' consent to the use of their records.

Version 5

DOCUMENT NUMBER	**STHK0117**
APPROVING COMMITTEE	Risk Management Council
DATE APPROVED	01 June 2018
DATE IMPLEMENTED	01 June 2018
NEXT REVIEW DATE	30 June 2021
ACCOUNTABLE DIRECTOR	Director of Informatics
POLICY AUTHOR	Head of Information Governance & Quality Assurance – Data Protection Officer
TARGET AUDENCE	All Staff
KEY WORDS	GDPR, Confidentiality, Data Protection, Email, Internet, Facebook, Twitter, Acceptable
Key Changes	**May 2018**: **Code of Confidentiality** • Executive summary – updated the fine details from the ICO and included a line about recording incidents on Datix • P9 – Updated the section on various Acts • P10 – Updated the items defined as personal information • P11 – 4.11 – special category data updated • P20 – updated the section on Police requests, as the request still has to be formal and approved by the Caldicott Guardian, but is not a Section 29 as previous in the Data Protection Act 1998 as the exemption to disclose for the prevention and detection of a crime.

	• P23 – Updated the list of secure email addresses from sthk and this item is updated in the training slides also. • P27 – Password information is correct in line with current process and training. • P31 – Updated removable media items • P35 – Item 7.26.1 – Updated the section around children and young people with capacity as it is confirmed that the age for consent for processing is reduced to 13. I have included a statement in this section around Gillick competency. Included a section from the Data Protection Act Article 8(1) outlines the changes around child consent which was around reducing the age of consent for processing from 16 to 13. I've also included a statement from ICO advising that children have the same rights as adults over their personal data. There is also a statement about consideration for subject access requests for this vulnerable group with the legal team liaising with Safeguarding as appropriate. • P41 + 42 – under 7.33 Year on Year improvements includes an update on the new toolkit. • GDPR and DPA 2018 has been updated throughout the document.

Important Note:

The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as "uncontrolled" and, as such, may not necessarily contain the latest updates and amendments.

Contents

EXECUTIVE SUMMARY

Any organisation that processes personal information faces severe consequences for failing to maintain appropriate confidentiality and security. This includes fines of up to €20,000,000 for breaching the Data Protection Act, and/or significant reputational damage.

Do...

- Inform patients about how we use their information.
- Share relevant patient information with those supporting patient care.
- Ask patients at every attendance to tell us their current address and GP, and update our systems if necessary.
- Adhere to records retention and disposal policies and procedures.
- Report breaches of confidentiality to the Information Governance Team.
- Record incidents on Datix.
- Transfer information in a safe and secure manor

Don't...

- Share more personal information than is necessary for the purpose.
- Access patient records of friends, colleagues or relatives
- Use identifiable personal information if the purpose can be satisfied by using anonymised data.
- Ignore breaches on confidentiality; report them.
- Use personal devices to transport or handle patient or staff information
- Misuse Social Networking Sites by posting inappropriate comments or images online
- Feel pressured to disclose information to the Police; staff should refer them to the Information Governance team

1. Scope

All NHS employees are bound by a legal duty of confidentiality to protect person identifiable information that they may come into contact with during the course of their working day. This is not just a requirement of their contractual responsibilities, but also a requirement within the Data Protection Act 2018 and the Common Law Duty of Confidentiality. In addition, Health Professionals have standards laid down in their own Professional Codes of Conduct.

Employees are required to keep person identifiable information relating to patients or staff, strictly confidential. Person identifiable information is not only found in a patient's health record it may be recorded in personnel records, databases, waiting lists, referral letters, discharge summaries, invoices etc.

The Trust has four main aims with regard to Confidentiality these are to:

- **Protect** – keep person identifiable information secure from unauthorised access
- **Inform** – ensure that all patients are aware of how their information is used
- **Provide Choice** – allow patients to decide whether their information can be disclosed or used in particular ways
- **Improve** – always look for better ways to protect, inform, and provide choice to the individual.

The purpose of this policy is to re-enforce St Helens and Knowsley Teaching Hospitals commitment to Information Governance.

The Trust recognises the importance of reliable information, both in terms of clinical management of individual service users and the efficient management of services and resources. Information Governance plays a key part in supporting Clinical Governance, Service Planning and Performance Management.

This Policy sets out the principles by which the confidentiality integrity and availability of person identifiable and corporate information will be managed within the Trust whether this information is stationary or in transit. This policy provides staff with clear guidance on how to manage the different forms of information and clarifies their roles and responsibilities.

This Policy also covers the use (and conduct associated with that use) of social media sites, applications and software, email and internet usage both while at work and outside of work, and associated disciplinary procedures.

2. Introduction

Information Governance provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of information, allowing:

- Implementation of central advice and guidance
- Compliance with the law
- Year on year improvement plans

Information Governance also gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

The Trust will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Digital Data Security and Protection Toolkit.

This document is a guide to ensure the required practice is followed for those who work permanently or temporarily within, or under contract to St Helens & Knowsley Hospital Trust concerning the confidentiality of person identifiable information. This code includes person identifiable information concerning patients and employees and should be seen as a key component of Information Governance within the organisation. This code of conduct should be read in conjunction with the Trusts Information Governance Policy, Freedom of Information Policy, Network, Information Security and Risk Policy, Mobile Device Policy, and Records Management Policies

NHS organisations are required to establish best working practice that effectively delivers the confidentiality that is owed to person identifiable information by the application of the law, ethics, and policy.

3. Policy Objectives

The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisations. All staff working for, and on behalf of St Helens & Knowsley Teaching Hospitals NHS Trust, (hereafter referred to as the Trust), must also meet these legal requirements. It is essential therefore, that staff understand what they need to do to keep information safe and secure

Staff should consider all information to be sensitive and apply the same standards to all information they come into contact with.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

Information Governance is the way in which the NHS handles all organisational information. It pulls together all the information handling requirements into one framework – in particular the personal and sensitive information of patients/service users/clients and staff. It allows organisations and individuals to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to protect confidentiality and assist in the delivery of the best possible services and care.

It is vital that when staff, other Trusts or external agencies are required to send personal or sensitive information into a Trust department, they are confident that the documentation is being sent to a location that ensures the security of the data and that the method used for delivery or a response is of a suitably secure standard.

The awareness and behaviour of staff members is the most important element in any organisation's information security therefore this policy:

- Staff must make sure that any personal information about patients/service users/clients and staff, that you hold or control, is effectively protected at all times against improper disclosure/loss. Many disclosures/losses are unintentional and avoidable.
- Ensure that errors give rise to learning – lessons can usually be learnt from errors allowing good practice for the future
- If there is an error; report the incident to the Information Governance Office and record the incident on Datix, the Trust incident and risk management system.
- Share your good practice - if you identify ways in which information handling can be improved in your work area share your ideas with your colleagues.
- Encourage others to share their good practice.
- Promote teamwork being the key to ensuring that all personal information is treated with respect and with regard for confidentiality.
- Ensures that all staff within the Trust are aware of their responsibilities whilst using social networking sites;
- Refers to all user activity in relation to e-mail, and the internet;

Basic Principles

To enable St Helens and Knowsley Teaching Hospitals NHS Trust and its staff -

1. To hold information securely and confidentially.
2. To obtain information fairly and efficiently.
3. To record information accurately and reliably.
4. To use information effectively and ethically.
5. To share information appropriately and lawfully.

- Any personal information given for one purpose must not be used for another purpose without the consent of the individual concerned as it may breach confidentiality
- An individual's right to confidentiality is protected by law
- Individuals have the right to know what information is being collected and why, and the reasons for sharing that information
- In some circumstances an individual has the right to choose how their personal information is to be used or who is allowed to see it
- Every member of staff has an obligation to:
    - protect confidentiality
    - ensure that any person asking for another's information is authorised to have access to it
    - understand their responsibility in relation to confidentiality
    - understand and follow the Trusts policies relating to confidentiality.

REMEMBER - That to wilfully/deliberately breach confidentiality, or any of the Trusts policies which are in place to protect person identifiable information, will result in disciplinary action (Disciplinary Policy and Procedure) being taken by the Trust and could potentially lead to dismissal.

It is important that staff understand that disclosure and sharing of personal identifiable information is governed by the requirements of certain Acts of Parliament, and Government and NHS guidelines. These include:

- General Data Protection Regulation
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- Common Law duty of Confidentiality
- The Children's Act 1989 & 2004
- Health & Social Care Act 2012
- Records Management Code of Practice for Health & Social Care 2016
- The Human Rights Act 1998
- Caldicott Report & Principles
- The Freedom of Information Act 2000
- Access to Health Records Act 1990
- Crimes and Disorder Act 1998
- Public Interest Disclosure Act 1998
- Information Security NHS Code of Practice Police and Justice Act 2006

This Code has been designed to provide guidance to employees and raise awareness of the procedures that will protect them from causing any inadvertent breach of confidentiality

4. Definitions

This policy covers all aspects of information within the Trust including (but not limited to):

- Service User information
- Personnel Information
- Organisational Information

This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems – paper and electronic
- Transmission of information – fax, e-mail, post and telephone

This policy covers all information systems purchased, developed and managed by or on behalf of the Trust and its partners, including any individual directly employed or otherwise by the Trust.

4.1. Person Identifiable Information

Person identifiable information can relate to patients, employees, (including temporary or bank employees), student placements, and medical students.

Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that employees will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence.

It is essential, if the legal requirements are to be met and the confidence of patients and employees is to be retained, that the Trust provides, and is seen to provide, a confidential service.

Person identifiable information is anything that contains the means to identify an individual and may consist of one or more of any combination from the examples listed below:

- name
- date of birth
- sex
- address
- location data
- online identifiers
- postcode
- telephone number
- visual images
- identification numbers

Certain categories of information are defined as sensitive information for which the law makes further provision i.e.

- political persuasion
- religious beliefs
- Sexually transmitted disease
- diagnosis
- sexual orientation
- HIV
- In-vitro fertilisation

Person identifiable information may be held on paper, CD, in computer files or printout, video, photograph, audio tape or heard by word of mouth.

It includes information stored on, or in computers on secure network drives, manual files or portable devices, such as encrypted laptops and encrypted USB drives. Any images or data taken on a mobile device such as a digital camera must be saved and stored securely on a network drive with role or person based access.

4.1.1. Sensitive Personal Information:

Sensitive personal information is defined as special category data of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or the wider community, for example, where the personal information contains details of the individual's:

- Race;
- Ethnic origin;
- Political opinion;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where this is used for identification purposes);
- Health data
- Sex life or
- Sexual orientation
- Criminal convictions

4.2. Confidential Information

Confidential information can be anything that relates to service users, staff (including non-contract, volunteers, bank and agency staff, locums, and student placements), their family or friends, however stored.

For example, information may be held on paper, CD, computer file within a secure network drive with role or person based access, printout, video, photograph, tape, any electronic portable media or even heard by word of mouth.

It includes information stored on portable devices such as laptops and memory sticks/USB devices. These devices must be encrypted to reduce the risk of a potential data breach if the items are lost or stolen. Any removable device such as a memory card for a digital camera must NOT contain any patient identifiable images. All images must be stored on a secure network drive with the relevant role or person based access permissions granted to view that information.

It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes Trust organisation confidential information.

During your duty of work you should consider all information to be sensitive, even basic demographics such as a name and address. The same protective standards should be applied to all information you come into contact with. Off-duty the same standards apply as you should not discuss work outside your place(s) of work even with other NHS staff or close family as this can be overheard, recorded, etc.

4.3. Safe Haven:

The term ‘safe haven’ is used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the principles laid out in this policy.

4.4. Principles of Information Governance

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability but equally places importance on the confidentiality of, and the security arrangements to safeguard both personal information about service users and staff and commercially sensitive information.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality healthcare. As such, it is the responsibility of all Clinicians and Managers to ensure and promote the quality of information and to actively use information in decision making processes.

4.5. Instant Messaging Software

IM is a form of text-based communication from one person to another that allows users to chat back and forth in real time. IM can make a user’s computer vulnerable to Denial of Service (DoS) attacks and may leave the IT infrastructure open to potentially harmful software or virus attack via file transfer. Only approved Instant Messaging Software maybe used on corporately issued devices.

5. Legal Implications

For a full list of legal implications please see Appendix C.

6. Duties Accountabilities and Responsibilities

6.1. Chief Executive

The Head of the Organisation has overall responsibility for the strategic and operational management of the Trust including and ensuring that Trust policies comply with all legal, statutory and good practice guidance requirements.

6.2. Director of Informatics (Senior Information Risk Owner)

The Director of Informatics has delegated responsibility for managing patient confidentiality and ensuring effective implementation and monitoring of this policy document. In addition the Director of Informatics will provide advice to the Chief Executive in regard to any information risk and will provide assurance of compliance with this policy and inform the Board regarding information security risks and how they are managed.

The Senior Information Risk Owner (SIRO) takes overall ownership of the Organisation's Information Risk Policy, and acts as the champion for information risk on the Board and provides written advice to the Chief Executive on the content of the Organisation's Statement of Internal Control in regard to information risk.

The SIRO is expected to understand how the strategic business goals of the Organisation and how other NHS Organisations' business goals may be impacted by information risks, and how those risks may be managed.

The SIRO will implement and lead the NHS Information Governance (IG) risk assessment and management processes within the Organisation and advise the Board on the effectiveness of information risk management across the Organisation

6.3. Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that the Trust processes satisfy the highest practical standards for handling patient information and provide advice and support to Trust staff as required.

The role of the Guardian is to safeguard and govern uses made of patient information within the Trust, as well as data flows to other NHS and non-NHS organisations. Caldicott Guardianship is a key component of broader information governance.

The Guardian is responsible for the establishment of procedures governing access to, and the use of, person-identifiable patient information and, where appropriate, the transfer of that information to other bodies.

The Guardian utilises the Department of Health publications to assist him in embedding the Caldicott principles within the Trust. This document sets the

role of the Caldicott Guardian within an organisational Caldicott/Confidentiality function which is itself a part of the broader Information Governance agenda.

The Trusts Caldicott Issues Log will be held on a secure area of the Trust network. Regular Caldicott Issues Log reports will be presented to the Trust Information Governance Steering Group. Both the Caldicott Guardian and the SIRO will be assisted in their work by a comprehensive support structure.

6.4. Head of Information Governance

The Trust's Head of Information Governance is the Data Protection Officer and Freedom of Information lead and the role includes:

- Maintaining Data Protection Register entries;
- Ensuring adequate training is provided via the Information Governance Training Tool; and
- Acting as initial point of contact for any data protection and freedom of information issues which may arise within the Trust.

6.5. Information Asset Owner/ Information Asset Administrators

Each computer system/database will have a designated system owner, called an Information Asset Owner, and system administrator, called an Information Asset Administrator. These may be part of the same role or separate. A list of these nominated personnel will be maintained by the Information Security Officer. It is the responsibility of these personnel to keep the Information Security Officer Informed of any changes in system use or personnel.

The Data Protection Officer and the Information Security Officer will ensure that all databases that require registration are registered in accordance with the Act's requirements and these registrations are reviewed on a regular basis.

The day-to-day responsibilities for enforcing the policy will be devolved to the Information Asset Owners and the Information Asset Administrators. The Information Security Officer will provide advice and guidance on the most effective way of ensuring adequate information security and confidentiality.

Staff will give due recognition to the sensitivity of person-identifiable information (relating to patients, carers, staff and others) and the need to maintain confidentiality. They will observe the requirements of their professional codes of conduct, the Caldicott principles and the various Codes of Practice for handling information in health and care.

6.6. Directorate/Operational Directors and Senior Managers

The Directorate/Operational Director is responsible for ensuring that all directorate staff are aware and implement Information Governance policies including this policy, procedures, standards.

6.7. The Information Governance Team

The Information Governance Team is responsible for advising on strategic direction, the development of policy and guidance for the Trust, and also operational support to the Trust on Information Governance compliance.

6.8. Information Governance Steering Group

The Information Governance Steering Group is a standing committee accountable to the Trust Board via the Risk Management Council. Its purpose is to support and drive the broader Information Governance agenda and provide the Trust Board with the assurance that effective Information Governance best practice mechanisms are in place within the Organisation

6.9. Human Resources Department

The Human Resources department will inform the Informatics department of all starters, leavers and assignment changes to ensure that new starters, staff moving within the organisation, and leavers will be processed swiftly. Additionally, reports must be provided by HR detailing changes to personnel so that the systems can be kept as secure as possible by limiting access only to those that need it to perform their roles.

6.10. Staff

All staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the Information Governance requirements including confidentiality and ensuring they comply with these on a day to day basis

A full list of staff responsibilities around e-mail and internet use is shown in Appendix B.

7. Processes

7.1. Confidentiality Code of Conduct Policy Processes

There are four key inter-linked strands to the Confidentiality Code of Conduct Policy:

- Openness
- Legal compliance
- Information security
- Information quality assurance

7.1.1. Openness

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

- Non confidential information on the Trust and Services are available to

the public via The Freedom of Information Act 2000 publication scheme.

- Service Users will have access to information relating to their own healthcare, options for treatment and their rights as service users. There will be clear procedures and arrangements for handling queries from service users and the public.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media. Staff will in the first instance direct these inquiries to the Media, PR and Communications Department.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.
- The Trust regards all identifiable personal information relating to service users as confidential, compliance with legal and regulatory frame will be achieved, monitored and maintained. This will be monitored by the Information Governance Steering Group on a monthly basis via the Trusts Data Security and Protection Toolkit submission, updates on the progress of this will delivered quarterly.
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act, Human Rights Act, The Common Law duty of confidentiality and the Freedom of Information Act. These policies can be located from the Trust Intranet.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided. This will be assessed through spot checks and visits to wards and departments, where it is identified that areas/individuals who require further training, support or guidance this will be provided by the Information Governance Team.
- Risk assessments, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable Information Governance controls are in place. Risk assessments will be conducted by the IAO in conjunction with the Trusts Information Security Officer.

7.1.2. Information Governance Framework

St Helens & Knowsley Teaching Hospitals NHS Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about service users and staff and commercially sensitive information necessary for the operation of the trust.
The Trust also recognises the need to share patient information with other health organisations and agencies in a controlled manner consistent with the

interests of the service users and, in some circumstances, the public interest.

It is important that information about identifiable individuals (such as patients and staff) should only be disclosed on a strict need-to-know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

The Trust believes that timely, accurate and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians, professionals and managers to ensure and promote the quality of information and to actively use information in decision making processes.

7.1.3. Freedom of Information

- Non confidential information about the Trust and its services will be available to the public through a variety of media and the Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of the freedom of Information policy and arrangements
- Service users will have ready access to information relating to their own health care; their options for treatment and their right as patients.
- The Trust will have clear procedures and arrangement for liaison with the press and broadcasting media (These will be held locally by the Media PR and Communications Department)
- The Trust will have clear procedures and arrangements for handling queries from patients and the public.

The Trust is committed to openness and transparency and as a result complies with the Information Commissioners Office model publication scheme were we make as much information available to the public using our Internet as the vehicle for delivery.

7.1.4. Information Security

- The Trust will establish, implement and maintain policies for the effective and secure management of its information assets and resources.
- Audits by Mersey Internal Audit will be undertaken or commissioned to assess information and IT security Assurance
- The Trust's Incident Reporting system will be used to report, monitor and investigate all breaches of confidentiality and security
- The Trust will promote effective confidentiality and security practice to its staff through its Information Governance policies, procedures and training. These policies and procedures are available on the Trust Internet and from the Information Governance team.
- The Trust will use ISO27001 Information Security standard as the basis of its Information Security management arrangements

7.1.5 Information Quality Assurance

The Trust will establish and maintain policies for Information Quality Assurance and the effective management of records. Audits will be undertaken or commissioned of the Trust's quality of data and records management arrangements.

Managers will be expected to take ownership of, and seek to improve, the quality of data within their services.

Wherever possible, information quality assurance will be assured at the point of collection.

The Trust will promote data quality through policies, procedures/user manual and training.

7.2. Keeping Information Secure

Employees working in departments where medical, personnel or corporate records are used must:-

- Shut/lock doors and or cabinets where records are kept.
- Wear ID badges.
- Query the status of strangers.
- Report anything suspicious or worrying to their department line manager
- Never divulge how the Trust security systems operate
- Not breach security (ref Trust Network, Information Security and Risk Policy)

7.3. Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, using the Trust record tracking procedures
- Returned to the filing location as soon as possible after use
- Stored securely whilst temporarily required within any clinic or office, so that the record can be located if needed urgently
- Stored closed when not in use so that contents are not seen accidentally
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons
- Held securely within the Department

Staff must not use public transport, which includes the hospital shuttle bus to transport patient or staff information please contact the Health Records department who will provide a driver.

7.4. With electronic records employees must:

- Never look, copy, download or make any unauthorised use of any clinical or personnel information relating to their family, friends, patients or people in the public eye, who are treated by the Trust. Access to clinical, information is only acceptable if you are directly involved in the clinical care of a patient.
- Always log out of any computer system or application when you leave your desk or no longer need access.
- Not leave a terminal unattended and logged in.
- Not share logins with other people. If other employees have need to access, then this will be organised for them upon application to the Informatics Department – not by using somebody else's user name or password.
- Not reveal passwords or share smart cards with other members of staff.
- Change passwords at regular intervals when prompted, or if your password might have been compromised.
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children or pet names or birthdays). Further information on passwords management is available from the Informatics Department.
- Where possible it is best to protect the monitor view to avoid patient's information being seen.
- Not save any work that contains person identifiable information to a shared drive where it would be accessible to unauthorised users.

7.5. Verbal communication:

- A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality, particularly in modern open plan offices. Care should be taken to ensure that confidentiality is maintained in such discussions.
- Where information is to be shared by phone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant telephone number, double checking that it is the correct number for that individual / organisation and then calling the recipient back.
- Where information is transferred by phone, or face-to-face, care should be taken to ensure that personal details are not overheard by other staff who do not have a "need to know". Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts, etc.
- Messages containing personal information should not be left on answer machines.

7.6. Requests for Person Identifiable Information

- Never give out information regarding patients/employees, to persons other than those who have a justified 'need to know' and have been 'authorised to access'. Those who 'need to know' are usually involved in the immediate health care and treatment of that Patient
- Always check the identity of the person requesting the information.
- Check the identity of telephone requesters by calling back using an independent source for the phone number
- All requests for identifiable information should be on a justified 'need to know' basis.
- Only the minimum necessary information should be given
- Follow existing 'Information Sharing Protocols'
- Some requests may need to be agreed by the Caldicott Guardian or Trust procedures as in the case of research.
- If in doubt ask a health professional or your line manager

7.7. Requests for information - Police or Media

7.7.1. Media

All Media requests and calls should be referred to the Media, PR and Communications Department.

7.7.2. Police

Under data protection law the police or other enforcing public agencies must provide a formal request for information under the Data Protection Act 2018 Schedule 2(1) and GDPR 6(i)(d). (This has replaced the previous Data Protection Act 1998 Section 29 (3) form).

This sets out the legal gateway for the request, e.g. to assist in the prevention or detection of a crime, prosecution or apprehension of offenders, or those protecting the vital interests of a person. (Being a missing person isn't a crime)

Note that it is still the Trust's decision at its risk whether to disclose, it isn't compulsory.

If the request is about any other matter or if in doubt contact the Legal Services Department before providing any information.

7.8. Disclosure to other Employees

Information concerning patients/employees should only be released to other employees in the Trust if they have the access rights to that information

- Always check employees have a justifiable need to access the information
- Check they are who they say they are via their ID Badge or internal extension number

- Don’t be bullied into giving the information

7.9. Carelessness

- Do not talk about patients in public place, or where you can be overheard.
- Do not leave any medical records or confidential information lying around unattended.
- Make sure that computer screens are not visible to the public or facing windows.
- Whiteboards/Chalkboards should not display any person identifiable data.
- Clinic lists should not be left in rooms especially those accessible to the public.
- Remove all paperwork used in meetings from the room after use.
- Do not pin any patient lists or documents on walls.
- Personnel/employees records should be kept in a locked room and locked cabinet.

7.10. Disposal of Confidential Documents & Removable Media

Disposal of documentation other than those to which retention schedules apply should be by safe and designated means.

- Always use the confidential disposal bins provided by the organisation
- Never tear up confidential documentation and put in waste paper bins
- Never throw confidential documentation or plastic bags filled with the same into council refuse bins.

Contact the Informatics Department to dispose of CD’s, memory sticks or any computer equipment that contain confidential information.

All Trust equipment that requires decommissioning must be done so through an approved company that can provide a ‘Certificate of Destruction’.

7.11. Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be:

- Specifically addressed to a named recipient never to a department, or a unit of an organisation
- Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked “Personal and Confidential to be opened by the recipient only”.
- The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.

- If an organisation has a policy that all mail is to be opened at a central point this policy must be made clear to all partners. An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know.
- The personal information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.

7.11.1. Internal mail

Confidential data must be sent in a secure sealed envelope, and marked accordingly e.g. 'Confidential' or 'Addressee Only'

7.11.2. External mail:

Should also follow the guidance above. Special care should be taken with personal information sent in quantity, such as copies of case notes requested by Solicitors or through subject access requests. Special care should be taken with the packaging and addressing and transfers of such information should be sent by recorded delivery to ensure that it arrives at the correct destination.

Patient identifiable information must not be copied and transferred onto removable media without prior approval from the Director of Informatics or suitably authorised deputy and must be encrypted to NHS standards (contact the Helpdesk) and should only be sent by recorded delivery or by the Trust approved courier service. It is advisable to obtain a receipt as proof of delivery e.g. copy of patients records to a solicitor.

Personal identifiable information or information that is deemed sensitive to the Trust must not be sent to or from staff or third party personal email accounts, e.g. – gmail, Hotmail etc.

7.12. E-mail, Encryption and Sending Sensitive Information

Any emails containing personal identifiable data or sensitive data must be placed in a password protected Word or excel document.

The document should then be attached to the email. It is vital that staff remember to ask the person receiving the email to phone the sender when received for the password. The password must not be included in the email. This is to safeguard you if the email is sent to the wrong address.

If you are sending the email from a @sthk.nhs.uk address to any of the following it does not require encrypting;

5bp.nhs.uk	hsthpct.nhs.uk	onehalton.org.uk	sthk.nhs.uk
GP-N81066.nhs.uk	knowsley.nhs.uk	shk.nhs.uk	sthkhealth.nhs.uk
haltonccg.nhs.uk	knowsleyccg.nhs.uk	sthelens.nhs.uk	wbhospice.org.uk
haltongp.nhs.uk	knowsleypct.nhs.uk	sthelensccg.nhs.uk	willowbrookhospice.org.uk
his.sthk.nhs.uk	nwbh.nhs.uk	sthelenspct.nhs.uk	wshospitalscharity.org

If you are sending from a @sthk.nhs.uk to any other email addresses it must be encrypted.

Sensitive personal information that identifies a service user or member of staff, or commercially sensitive information must not be sent by e-mail (.nhs.uk) unless it is encrypted to NHS standards.

After attaching your password protected document just simply type **[ENCRYPT]** in the subject line of the email and the system will enforce encryption. The person receiving the email will then be required to register to use the system with their email address. The process will take them approximately 90 seconds. Remember to ask the person receiving the email to phone you when the email is received for the password.

If you have an NHSmail account that ends in @NHS.net you can securely send emails from that account to the following addresses without added encryption;

- *.gcsx.gov.uk for local government
- *.gsi.gov.uk and *.gsx.gov.uk for central government
- *.cjsm.net and *.pnn.police.uk for Police/Criminal Justice
- *.mod.uk for Ministry of Defence

Staff must never send patient identifiable information to any personal email address.

Staff must never send sensitive information from their personal email account to their Trust email account.

The amount of time that an employee may use the e-mail system for reasonable personal use should be agreed with their line manager.

Copyright in all documents created via e-mail is the property of the organisation and not the individual user.

E-mails sent by a Trust employee are the organisations property. Unless such e- mails are marked Personal in the 'Subject Field' they may be opened by the Trust.

E-mail (unless marked Personal in the subject field) is considered corporate correspondence and as such is accessible under the Freedom of Information Act 2000. It is therefore important to save e-mails that have been used to formulate corporate decisions, policy, or procedure, as they may be subject to a request. These e-mails should be referenced, saved and retained to appropriate record retention periods following advice from the organisations Head of Information Governance.

Employees must not share their password and user name with any other person and should not leave their computers unattended whilst logged on, as they will be held responsible for any activity, which takes place using their account.

Unauthorised use of someone else's identity to send or intercept e-mail is strictly forbidden and will result in disciplinary action.

Employees must not distribute any material by e-mail which is:

- unlawful,
- objectionable
- causes offence, examples of which include but is not limited to offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability
- contains material which is libellous or pornographic includes incitement to commit a crime, hatred and violence or any activity that contravenes any of the Trust's Policies including Equal Opportunities Policy.
- Material that could be abusive, indecent, obscene, menacing; or in breach of confidence, copyright, privacy or any other rights.

Any member of staff who receives e-mail containing material which is in breach of this policy should inform their line manager immediately, who will institute the organisations incident reporting procedures.

Distribution of such material may result in legal action and/or disciplinary procedures. The Trust reserves the right to monitor e-mail usage.

Where a member of staff receives e-mails from unsolicited sources the sender should be added to their personal 'Blocked Sender List'. (Contact the Helpdesk for information).

Where there is any doubt about the origin of an email or its attachments staff must contact the Help Desk for advice as viruses can be spread through e-mail and the opening of suspect attachments may result in loss of or damage to the Trust IT systems.

Users should exercise caution when disclosing their work e-mail address to commercial organisations, as this information may be passed to other 3rd party organisations generating 'junk' mail.

Employees must not use the organisations e-mail system to conduct any personal business enterprise.

It is inappropriate to forward or create chain letters to other e-mail users either within the organisation or externally. If a user receives a chain letter that has inappropriate content they must inform their line manager who will instigate the organisations reporting procedures. Staff must also ensure that they do not click on links and attachments, from people they do not know, or that are contained within SPAM emails.

To avoid inappropriate content being circulated users should not set their e-mail to "auto forward" (Contact the helpdesk for information)

Only those employees who are specifically authorised to give media statements on behalf of the Trust, i.e. the Media, PR and Communications Department, may write or present views, concerning the Trust and its business, via e-mail.

7.12.1. E-mail – Monitoring

The Informatics Department retains copy of all internal and external e-mail which is received or sent. The Department will not use this facility to monitor individual employees e-mail traffic without written permission or unless they have a justified need to monitor or investigate an employee's e-mails.

The Informatics Department will investigate inappropriate activity on behalf of the Trust under the following circumstances:

- a report of or concern raised about the contents of a computer
- a report of inappropriate or unreasonable personal use of e-mail or the Internet
- routine monitoring identifies potential inappropriate use

This list is not exhaustive.

The Informatics Department reserves the right to carry out detailed inspection of any IT equipment without notice, where inappropriate activity is suspected. A more detailed investigation may involve further monitoring and examination of stored data including employee deleted data held on servers, disks, drives or other historical/archived material.

Access to the content of an employee's mailbox in their absence, other than for the monitoring purposes already referred to, will only be granted on submission of a written request from a Senior Manager of the Trust area concerned to the Informatics Service Desk for approval by the Information Security Officer. This request must identify the business need for the access requested and indicate the mail message(s) required.

In the event of a user being absent from work for an extended period of time, access to their inbox may be granted to their line manager. The Informatics Department has a structured level of governance regarding granting access to e-mail records. Ultimate responsibility for this lies with the Data Protection Officer, when absent this responsibility is passed to the Deputy Director of Informatics.

The Informatics Department will only initiate a request for access to an individual's mailbox when a request for this access has been made in writing from the Senior Manager via the Informatics Service Desk to the Information Security Officer.

7.13. Internet Access & Monitoring

Access to the internet or external web resources will be authenticated by user name and password.

The time of day that staff may use the internet for reasonable personal access should be agreed with their line manager but as a general rule staff should not exceed 1 hour per day for non-work related Internet browsing.

Internet users must be aware that the internet is inherently insecure and confidential information in relation to the business of the Trust and/or service user/another staff member's identifiable information must never be disclosed or placed on internet sites or chat rooms. Although the Informatics department has put anti-virus defences in place, great care should be taken when using the internet. The Helpdesk should be informed where any suspicion of virus infection arises; the incident will be dealt with in accordance with information security procedures.

Downloading or distribution of copyrighted material without permission of the copyright holder, or of software for which the user does not have a legitimate license, is forbidden, this applies to any download for work or personal use.

The installation of downloaded software onto Trust computers, including laptops, is not permitted. The Informatics department should be contacted for the installation of any required software. Information downloaded for personal use must not be stored on the Trust Network

The use of computers connected to other networks (including peer-to-peer networking systems) to download files or software is forbidden as is the installation of any such system or software on Trust computers.

Access to the internet is authenticated and logged on a user basis. Details such as the date and time of access, and the site visited, are recorded and the information is retained for one month and then archived. Further reports will be available for use when investigating an incident; these reports will only be disclosed upon receipt of a written request from the Service Director in question.

7.14. Passwords

Users must always ensure:

- a minimum of 9 characters in length
- contain at least three of the possible character types
- changed at least every 90 days
- not reused within 24 months
- changed on first login where a new password is issued by IT
- ensure that no-one is able to see what is being typed in.
- Staff should be aware they must comply fully with this policy

Users must not:

- Passwords should not contain all or part of the username, your date of birth or any consecutively repeated characters
- Write your password down on paper, a sticker or post-it and stick it under your keyboard or to your screen. Diaries or notepads are also not a secure place to store passwords. Mobile phones/tablets are not a secure place to store passwords & account information (they are easily stolen, most are not encrypted and do not have a PIN/Password set).
- Share passwords as the audit trail is compromised- i.e. if the user recorded against a transaction (for example the update of the allergies field in a person's medical record) is not stated as a specific individual, then exactly who made the transaction cannot be determined. This is important when considering legal challenges to data records- i.e. in the instance of potential legal proceedings

.

In exceptional circumstances the length of the password characters will be reduced to a minimum of four. This will have to be approved by the Director of Informatics or his deputies.

If you discover someone is not complying with this policy you must report it directly to your line manager or to the Trust Information Security Officer.

Systems owners may remove your access to their systems if you are found in breach of this policy which may impact your ability to do your job.

7.14.1. Single Sign On (SSO)

The Trust utilises a single sign on solution which can automatically manage backend passwords enabling them to be set to the maximum length and complexity possible for each system. As these passwords are never known to the users this in turn will make the individual systems more secure. This functionality will be implemented with the rollout of Single Sign on.

7.14.2. Account creation & resetting of passwords

Line managers must complete a login request form on the intranet for the new starter detailing the systems and files they require access to, and the level of access.

IT Services will create an active directory account for the user after receipt of the new starter from HR and on receipt of the login request form from the line manager. The username will be sent out by email to the line manager. The password will be given to the user over the phone when they start and then prompted to change it the first time they log on.

Please note that the above only relates to accessing the Trust Network and specific systems such as EDMS, PAS etc. Such system specific access will only be granted upon the completion of the relevant documentation and training.

If a user has forgotten their password or their account has been locked out, then the user should contact the IT Service Desk. (Account reset queries should only be made by the person who the account belongs to). Checks will be made to verify that the user is who they say they are and then the account can be unlocked or the password reset. Again the password will not be sent out in a message in clear text. Acceptable proof of identity can be the answer to a security question, or the service desk can contact switchboard and ask to be put through to the main departmental number and passed over to the user.

Users with single sign on can reset their password at the logon screen by answering three of the five security questions they answered when enrolled in the single sign on software.

All systems and applications (where possible) will be set up so that users will be forced to change their password at first time of logon after the creation of a new account or a password reset.

7.14.3. Generic passwords/accounts

Generic accounts are **not permitted within the Trust except** in exceptional circumstances and it is unavoidable (root & administrator accounts for example.)

Where possible these accounts will be subject to stricter password expiry rules, however a procedure must be in place so that when passwords are changed, users of these accounts are made aware (in a secure manner) and the old password is not entered, potentially locking the account.

7.15. Process for Safe Havens/Locations/Security Arrangements

When confidential information is received to a specific location in the Trust:

- It should be to a room/area that is lockable or accessible via a coded key pad known only to authorised staff.
- The room/area should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to all members of staff working in the same building or office, or to visitors.
- If the room/area is on the ground floor the windows should be lockable.
- The room/area should conform to health and safety requirements in terms of fire, flood, theft or environmental damage.
- Manual paper records containing personal information should be stored

in locked cabinets when not in use.
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use.
- Equipment such as fax machines should have a code password and be turned off out of office hours, (if possible).

In Summary; Safe Haven procedures should be in place in any location where large amounts of personal information is being received, held or communicated especially where the personal information is of a sensitive nature e.g. patient-identifiable information.

7.16. Process for Fax Machines

One of the most common breaches of confidentiality occurs when documents that contain patient identifiable information are sent by fax machine. Many fax machines are in corridors or open plan offices and are used by several different departments. Staff collect faxes but do not always check that all the pages belong to them; this increases the risk of information being seen by unauthorised persons.

To combat this, the Trust has identified certain fax machines as 'Safe Haven' machines. These are machines that are located in a secure area and are used to receive documents of a private and confidential nature. Staff must contact their line manager for details of their nearest safe haven fax machine and a front cover sheet must be used.

7.17. Social Networking Sites

Access to social networking sites examples of which are Facebook, Twitter, Instagram and Snapchat (this list is not exhaustive) is strictly prohibited from Trust owned/managed computer equipment unless approval has been given by the Trust Executive Committee or the Trusts SIRO to utilise social networking sites for the purpose of either communications or public information or to improve patient care

Access to social networking sites will only be considered for approval once a request has been made in writing from the Service Director to the Data Protection Officer or SIRO directly.

Staff must be aware that social networking sites make personal information publicly accessible, allowing people to upload to a profile with personal details, photos, videos and notes and to then link with their "friends" profiles. This raises immediate concerns about privacy.

Although individuals may believe they have restricted access of their profile to their "friend" list, the High Court ruled that all postings to social network sites are regarded as being in the public domain and as such potentially accessible to all.

Personal use of social networking sites may:

- Bring the organisation into disrepute by the posting of damaging remarks whether about St Helens & Knowsley Teaching Hospitals NHS Trust, patients, service users, colleagues or other 3rd parties.
- In line with BMA and GMC best practice guidance; staff should not 'friend' patients on Facebook, or any other social networking site.
- Give rise to risks of legal claims against the organisation, which is generally vicariously liable for the actions of its staff.
- As a consequence of inappropriate use of social networking sites staff might find themselves:
    a) Breaching this Policy
    b) Damaging the organisation's reputation in such a way as to constitute a breach of individual's employment contracts, leading to disciplinary action and possible dismissal.
    c) Breaching confidentiality, data protection, employment contract or professional Code of Practice

It is therefore vital that Staff who access or are members of social networking sites in a private capacity do not post images that have been taken inside of, in the grounds of, or of Trust premises, or place misleading, malicious, or derogatory comments or references that would damage the reputation of, or misrepresent the Trust, or cause distress to its patients, service users or any other employee.

Failure to comply will result in disciplinary procedures

Staff should be aware that the Trust monitors information posted about the Trust online (both generally and on social media sites) for content that it finds inappropriate or any associated breaches of this policy.

7.18. Cloud Storage Use

Cloud storage and file sharing website such as Dropbox are not allowed to be accessed due to the security and governance risks associated with these services. The Trust does not have the security mechanism and controls to safeguard information stored on Dropbox, or similar 'cloud' storage solutions; uploading personal/sensitive information on cloud storage services such as Dropbox puts the organisation's data at risk and exposes the organisation and its operation to:

- Malicious files
- Identity theft
- Blackmail
- ICO Penalties

Access to cloud storage is only permitted with specific authorisation and approval from the SIRO or equivalent.

7.19. Capturing Images of Patients

Images of patients must not be taken on personal cameras, computers or mobile phones by any trust employee or visitor.

Doing so seriously risks breaching patient confidentially and consent, as well as breaching the law on data protection and human rights

If you need an image for clinical reasons, contact Medical Photography or X-ray out of hours.

7.20. Patient Capturing Images

The use of personal cameras, including camera and recording facilities on personal mobile devices, by patients is strictly forbidden on Trust premises unless the patient has the explicit approval of a senior member of staff (ward manager or equivalent), as this could in inadvertently breach patient confidentiality.

Under no circumstances are cameras or such devices with that facility allowed in secluded areas such as toilets, bathrooms and treatment rooms.

The Trust realises there will be certain occasions were patients would like to use their personal devices to record images, such as in maternity. In order to do so in a safe and secure environment the patient must seek the approval from a senior member of staff before capturing an image.

Personal cameras, including camera facilities on personal mobile devices, must not be used for any clinical purpose nor must they be used for the storing of clinical images however the clinical images were captured. Only Camera equipment purchased by the Trust specifically for clinical use may be used.

7.21. Removable Media/User Disks/USB Devices/ CDs & DVDs

Removable media can be defined as any portable device that can be used to store and move information. Media devices can come in various formats, including:

- Universal Serial Bus (USB) memory sticks (also known as flash drives)
- Compact disks (CD)
- Digital Versatile Disks (DVD)
- USB Hard Disk Drives
- Secure Digital Cards
- MP3 / MP4 players i.e. iPODs or any other brands
- Laptops, – iPADS, etc.
- Some mobile phones and digital cameras
- Dictation Devices

The Health Informatics Service Desk must be contacted to clarify the use of any other media devices not listed above.

Anything you can copy, save and/or write information to which can then be taken away and transferred or read on another computer, must **NOT** be used on Trust equipment, unless prior authorisation from the Health Informatics Service Desk has been given.

The above access and monitoring of such devices will be managed by the application of Trust Safend software.

Any databases other than legitimate Trust systems that contain patient/employees/ identifiable information should be password protected and should only be accessible to those who have been authorised to do so and should be kept on a secure 'drive'. Authority must be obtained from the Information Governance Manager to keep person identifiable information on a database other than approved system databases.

Identifiable information that is faxed should be pseudonymised. Where person identifiable information is to be sent via fax this must be done from and to a designated Safe Haven Fax. Recipient fax numbers should be pre-programmed into fax machines and regularly checked. If this is not possible the recipients fax number should be rechecked before the send button is pressed. Always remove information from the machine immediately after sending or upon receipt, and confirm receipt with the recipient. When faxing person identifiable information, follow Trust guidance located by Fax machines.

7.22 Record Keeping

7.22.1. Patient Records

Maintaining proper records is vital to patient care. If records are inaccurate, decisions that could potentially cause harm to the patient may be made. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors. The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that could lead to better treatments in the future. The practical value of privacy enhancing measures and anonymised techniques will be undermined if the information they are designed to safeguard is unreliable.

Patient's records should be factual, consistent and accurate and;

- Be written down as soon as possible after the event has occurred providing current information on the care and condition of the patient
- Be written clearly, legibly and in such a manner that they cannot be erased
- Be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly
- Be accurately dated, timed and signed or otherwise identified with the

name of the author being printed alongside the first entry
- Be legible on any photocopies
- Be written wherever applicable with the involvement of the patient or carer
- Be clear, unambiguous (preferably concise) and written in terms that the patient can understand. Abbreviations if used should follow common conventions
- Be consecutive
- Use standard techniques and protocols (for electronic records)
- Be written so as to be compliant with the Race Relations Act and the Disability Discrimination Act

Be relevant and useful

- Identify problems that have arisen and the action taken to rectify them
- Provide evidence of the care planned,the decision made, the care delivered and the information shared
- Provide evidence of actions agreed with the patient (including consent to treatment and/or consent to disclose information)

And include:

- Medical observations; examinations, tests, diagnosis prognoses, prescriptions and other treatments
- Relevant disclosures by the patient –pertinent to understanding cause or effecting cure/treatment
- Facts presented to the patient
- Correspondence from the patient or other parties

Patient records should not include

- Unnecessary abbreviations or jargon
- Meaningless phrases, irrelevant speculation or offensive subjective statements
- Irrelevant personal opinions regarding the patient (See Management of Health Records Policy available on the Intranet.

7.22.2. Staff Records

- Staff should never view their own, friends, family, colleagues or high profile patient's medical records. To do so would be a breach of this policy and could result in dismissal from employment. Access to clinical information is only acceptable if you are directly involved in the clinical care of a patient. An exception to this is if they have completed the necessary documentation via Access and Disclosure, Legal Services Department and have the necessary permission to do so
- Staff records should not be disclosed to a third party or used for a purpose other than the original intent without employees being informed, and consent given or where there is a statutory, legal requirement to disclosure.
- All employee records should be kept up to date and accurate.

- All employees records should be kept in accordance with the Human Resources Department procedures
- Subject Access to personnel records should follow the HR Department written procedures

7.23. Informing Patients effectively

Consider if patients would be surprised to learn that their information was being used in a particular way. If so then they are not being effectively informed.

To inform patients correctly employees should:

- Check, where practicable, that information leaflets on patient confidentiality and information disclosure have been given to the patient, read and understood.
- Make clear to patients when information is recorded or health records are accessed
- Make clear to patients who they are or who they will be disclosing information to.
- Check patients are aware of their choices, have no concerns, queries or objections concerning how their information is disclosed and used
- Answer any queries personally or direct the patient to others who can answer their questions.
- Respect the rights of patients including their right to have access to their health records through Trust Access to Health Records procedures.
- Refer patients to the leaflet 'How we use and Protect your Personal Information', should they require further information about how their personal and sensitive information is used. Should patients require further detail, staff should refer them to the Trust Information Governance team at IG@sthk.nhs.uk.

7.24. Provide Patients with choice

Patients have different needs and values – this must be reflected in the way they are treated both in terms of their medical condition and the handling of their personal information. Patients have the right to choose whether or not to accept a form of care and the information disclosure needed to provide that care, and to choose whether or not information that can identify them can be used for non-healthcare purposes.

Staff must:

- Ask patients before using their personal information in ways that do not directly contribute to or support the delivery of their care
- Respect patients decisions to restrict the disclosure or use of information except where exceptional circumstances apply
- Communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to, or restrict the disclosure of information. Record that decision in the patients notes

- Remind patients that they have the right to change their mind about a decision they previously made and if they do record that change of decision.

7.25. Research

Before conducting any research using person identifiable information employees must first seek approval from the Research Department and Ethics Committee (see Research and Development Strategy)

7.26. Consent and Capacity to Share Information

You owe a duty of confidentiality to all patients, past or present, even if they are adults who lack capacity. You may be asked to provide information from the medical records of patients who are incapable of giving consent, are aged under 18, or have died to agencies external to the Trust.

The below gives further information about dealing with these circumstances.

7.26.1. Children and young people with capacity

Many young people have the capacity to consent to the disclosure of their medical records. If the child or young person (under 18 years of age) is able to understand the purposes and consequences of disclosure (Gillick competent) they can consent or refuse consent to the disclosure. You should discuss disclosing the information with them and release it only with the child or young person's consent.

The Data Protection Act 2018 states in Article 8(1) of the GDPR (conditions applicable to child's consent in relation to information society services)— (a) references to "16 years" are to be read as references to "13 years", and (b) the reference to "information society services" does not include preventive or counselling services.

The ICO have issued guidance stating that children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

Consideration needs to be given therefore in instances for Subject Access Requests when a child is deemed Gillick/Fraser competent to disclose that data. Equally safeguarding needs to be considered for this vulnerable group, particularly when requests are made from parents/guardians for health information.

Collaboration is necessary between the Legal Team and Safeguarding Team when necessary to risk assess and determine the best course of action in terms of whether to disclose or not with the support from the Caldicott Guardian and Data Protection Officer.

7.26.2. Safeguarding Children and Young People up to their 19th Birthday

If a child or young person aged under 19 years refuses to consent to sharing their information with external agencies, you should nevertheless disclose the information if this is necessary to protect the child, young person or someone else from serious harm, or if disclosure is justifiable in the public interest.

The Children Acts of 1989 and 2004 and the statutory guidance, 'Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children and young people' (2010, HM Government) mandate the sharing of information in this situation whether the child is with or without mental capacity, as long as the information shared is proportionate, appropriate and in the child's best interests.

Examples include situations where you consider that the child or young person is at risk of neglect or abuse, the information would assist in the prevention, detection or prosecution of a serious crime, or where the child or young person may be involved in behaviour that might put themselves or others at risk of serious harm. It would also include a situation where a child or young person has refused to allow a carer to be told of a condition or treatment, from which there is a risk of a serious complication arising.

You should give careful consideration to the child's reasons for refusal of disclosure, and explain to them your reasons for disclosing the information and what you intend to disclose – unless doing so would undermine the purpose of the disclosure.

You should involve the child or young person in the decision and ensure this is documented – including notes on how the decision was reached.

7.26.3. Children and young people without capacity

The overriding principle, when dealing with the disclosure of the medical records of children or young people who do not have the maturity or understanding to make a decision, is ensuring that you act in their best interests.

If the child or young person lacks the capacity to consent to the disclosure of information, those with parental responsibility can consent on their behalf. The consent of only one person with parental responsibility is needed for consent for disclosure.

If you do not believe that the decision made by those with parental responsibility is in the best interests of the child or young person, and the disagreement cannot be resolved with discussion and mutual agreement, it may be necessary to seek the view of the courts.

In young people aged 16-17 who lack capacity, both the Mental Capacity Act 2005 and the Children Act 1989 can apply, depending on the circumstances. In England, the MCA defines anyone of age 16 as an adult. In relation to disclosure of information, the most important principle is to ensure that you are acting in the patient's best interests.

7.26.4. Adults lacking capacity

Any disclosure must be justifiable and the reasons for doing so must be fully documented.

The Mental Capacity Act 2005 applies to adults without capacity, and further details about the disclosure of confidential information about a patient lacking capacity can be found in the Mental Capacity Act Code of Practice. Under the Act, patients are assumed to have capacity, unless they have an impairment affecting their mind (e.g., dementia), which means they are unable to make a specific decision at a specific time. There is also a requirement to ensure all practical steps have been taken to help the individual make a decision.

The overriding principle is that the disclosure of confidential information is made in the best interests of the person lacking capacity. This may involve releasing information about their condition – for example, to their carer, to ensure they receive the best treatment.

If the patient has made a lasting power of attorney that covers personal welfare, you must consider the views of anyone who has legal authority to make a decision on the patient's behalf, e.g., a lasting power of attorney that covers personal welfare, or who has been appointed to represent them. Likewise, if the Court of Protection has appointed a deputy to make welfare decisions on behalf of the patient, that person must be consulted in relation to disclosures of confidential information.

7.26.5. Disclosure after a patient's death

Your duty of confidentiality extends beyond the patient's death. However, there may be circumstances when disclosure may be justified. For example, you are under a professional duty to respond to complaints, and this includes complaints made by bereaved relatives. Any disclosure must be justifiable and the reasons for doing so must be fully documented.

There is a Death Notification Procedure for all child deaths up to age 19 years that occur on Trust premises undertaken by the Paediatric Health Visitor Liaison team within the Trust (situated in the Paediatric Offices on Level 2) who notify all relevant agencies within the region according to regional procedure on the first working day following the death. This Death Notification Procedure can be found in the Paediatric Health Visitor Liaison's Standard Operating Procedures.

All child and infant deaths and deaths as result of a domestic homicide, irrespective as to whether they occurred within the Trust are subject to a Serious Case Review led by the deceased's respective Local Authority. If the deceased is known to the Trust, the Trust via the Adult or Children's Safeguarding teams is required to share detailed information in an Individual Management Review signed off by the Trust's Executive Lead for Safeguarding. The review can involve sharing information as part of the review process about the victim and other family members as requested by the leading authority. The Trust's Individual Management Review Completion Standard Operating Procedure can be found in the Trust's Safeguarding Children Policy and Standard Operating Procedures.

All sudden unexpected deaths in infancy (SUDI) and in children (SUDC) are subject to review by the Merseyside regional SUDI and SUDC protocols that require all agencies to share information. The SUDI and SUDC procedures are available in the Trust's Safeguarding Children Policy and Standard Operating Procedures.

Any request to disclose information for a Coroner's Inquest should be coordinated by the Trust's Legal Department. Trust staff asked to produce statements and reports for a Coroner's Inquest should submit their report/statement through the Trust's Legal Department and retain a copy themselves.

7.26.6. Who can you disclose information to?

You should consider whether disclosure would be justified in all the circumstances of the case.

The Access to Health Records Act 1990 applies to records of deceased patients, and to information recorded in or after November 1991. Under the Act, upon request, relevant information should be disclosed to the personal representative of the deceased (the executor of the deceased’s will or the administrator of the estate if your patient died without leaving a will) or anyone who may have a claim arising from the patient’s death.

If the request for disclosure is made by someone other than the personal representative or a person with a potential claim arising from the patient’s death, then, where possible, you should advise them to seek the consent of the personal representative. If this is not possible you should consider whether disclosure would be justified in all the circumstances of the case

7.26.7. What information can be disclosed?

If the patient has asked that specific information remains confidential, their views should be documented, and respected, subject to disclosures that are required by law or justified in the public interest. However, even in circumstances where you are not aware of any specific requests from the

patient, there are factors you should take into account before disclosing any information:

- Is it information which, by its nature, the patient might not have wanted disclosed?
- Could the disclosure of the information cause serious harm or distress to others?
- Would the disclosure inadvertently reveal information about a third party?
- Is the information already in the public domain?
- Is the disclosure necessary?

7.27 Information Sharing

Data Protection and Caldicott Principles must be applied to any proposed exchange of information before it takes place and guidance should be sought from the Information Governance Manager.

The Trust has adopted an Information Sharing Toolkit to manage information sharing with other NHS & non-NHS organisations. The Information Governance Manager will provide guidance and template Information Sharing Agreements where sharing is necessary upon request.

Further guidance should be sought from the Information Governance Manager or Caldicott Guardian before sharing.

Where a decision has been made that the sharing of information is justified and legal, all transfers of information must occur in line with this Policy and in conjunction with all of the Information Governance, Data Protection and Security policies.

To assist employees in making decisions on Patient consent to information sharing the Department of Health, in conjunction with the Information Commissioner, has developed a disclosure model that links with decision making flow charts: (see Appendix B1-3)

7.28 Acceptable Personal Use of email and internet & Disciplinary Procedures

St Helens & Knowsley Teaching Hospitals Trust allows limited personal use of the e-mail and internet system.

The Trust considers that staff may browse the internet or use e-mail within the boundaries of this policy for their own personal use prior to or after their normal working hours or during their lunch break.

Where there is a necessity to conduct such activities within working hours this should be agreed with your line manager.

The time of day that staff may use the internet for reasonable personal access should be agreed with their line manager but as a general rule staff should not exceed 1 hour per day for non-work related Internet browsing.

Any misuse of social networking sites which has a negative impact on the Trust - including what might be perceived as online bullying and harassment – may be regarded as a disciplinary offence.

The use of racist, homophobic, sexist or other prejudicial language by staff, including in e-mails or on the internet may also be regarded as a disciplinary offence. Staff should ensure they follow the Respect & Dignity at Work Policy when using Social Media sites.

7.29 Reporting Breaches

Employees should read this in conjunction with the Incident Reporting Policy. Employees should be aware of their responsibility to report any breach or risk to the confidentiality and/or integrity of information that they become aware of;

- Report breaches to your line manager and through the Trust Incident Reporting Procedures (Datix). If you feel that it would compromise your position you may report the breach, confidentially, directly to the Caldicott Guardian or Information Governance Manager
- Once a Line Manager has been notified of a breach they should report the incident immediately to the Caldicott Guardian or Information Governance Manager via Datix, giving details of the breach, date, time, place and any other relevant information
- Report any inadequate procedures that might lead to a breach
- There is specific legislation to protect individuals reporting any breach (contact the Human Resources department for further information) When dealing with a suspected or actual breach of information governance, staff should refer to the Information Governance Team

Suspected breaches of information governance must be reported to the Information Governance Team. Confidential reports of suspected breaches may be made via the Trust's Protected Disclosure of Issues of Concern Policy (Whistle-blowing).

7.30 Working at Home or elsewhere

It is sometimes necessary for employees to work at their own home. If you need to do this you would first need to gain approval from your manager. If they agree you would need to ensure the following are considered and remember that there is personal liability under the Data Protection Act 2018 and your contract of employment for breach of these requirements:

- Service user or staff manual records may not be removed from the Trust site(s) without managerial consent.
- Remote access into networked services must be strongly authenticated using a Trust remote access token (VPN)
- Ensure any personal information in portable electronic form is encrypted to prevent unauthorised access.
- While at home you have personal responsibility to ensure any records you may access are kept secure and confidential. You must not let any unauthorised person have any access to the records. This means that

- other members of your family and/or your friends/colleagues/visitors/ contractors must not be able to see these records or effect any access in your absence.
- If you work with any service user or staff records on portable electronic media you must ensure all of the above apply. In addition you must ensure such information is effectively deleted when you have finished your work. See the Trust's Mobile Working and IM&T security policies for further details

7.31 Abuse of Privilege

It is strictly forbidden for employees to look, copy, download or make any unauthorised use of any clinical or personnel information relating to their family, friends, patients or people in the public eye, who are treated by the Trust. Access to clinical, information is only acceptable if you are directly involved in the clinical care of a patient. This includes clinical records photographic or x-ray images or any other information held in any other media appertaining to the care of a patient/or employee of the Trust. Any member of staff found to be in breach of this principle will be subject to the Trusts disciplinary procedures and may be subject to Civil Action in the case of Data Protection breaches.

Employee should not attempt to bypass or defeat the security systems attached to Trust systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempt to breach the security of Trust electronic systems should be immediately reported to the Information Security Officer and would be considered a breach of the Computer Misuse Act 1990, Police and Justice Act 2006 and/or the Data Protection Act 2018.

7.32 Non Compliance

Non-compliance with this code of conduct by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust disciplinary procedure, and may lead to dismissal for gross misconduct (ref Disciplinary Policy and Procedure)

Examples of failure to comply with confidentiality responsibilities include, but are not limited to, deliberately looking at records without authority; discussion of personal details in inappropriate venues; transferring personal/sensitive information electronically without encrypting it, etc.

7.33 Year on Year Improvement

An assessment of compliance with requirements, within the Information Governance Toolkit (IGT), has been undertaken each year. From 2018/19 a new online mandatory self-assessment tool is available from NHS Digital replacing the Information Governance Toolkit with a more fit for purpose assessment, the Data Security and Protection Toolkit. Annual reports and proposed action/development plans will be presented to the Information Governance Steering Committee.

The requirements are grouped into the following initiatives:

- Personal Confidential Data [8]
- Staff Responsibilities [3]
- Training [5]
- Managing Data Access [3]
- Process Reviews [3]
- Responding to Incidents [4]
- Continuity Planning [2]
- Unsupported Systems [3]
- IT Protection [4]
- Accountable Suppliers [5]

8. Monitoring Compliance with this Document

Monitoring if compliance with this document will be overseen by the Information Governance Steering Group.

Key performance Indicators of the Policy

Describe Key Performance Indicators (KPIs) Must reflect	Frequency of Review	Lead
Duties are carried out as described in the policy	Annually	IG Manager
Compliance will be monitored via the Data Security & Protection Toolkit	6 Monthly	IG Manager
External Audit Rating to be of an acceptable standard.	Annually	IG Manager

Performance Management of the Policy

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
Refer to KPIs	Spot checks Website Feedback Mandatory Training DSPTool kit Reports External Audit Reports	IG Manager	As Above	IG Steering Group Risk Management Council Trust Board	Risk Management Council Trust Board
IG Mandatory Training	Training will be monitored in line with the Induction Mandatory and risk Management Training Policy.				

REFERENCES/ BIBLIOGRAPHY

Users will be obliged to comply with legislation as appropriate including:

- General Data Protection Regulation
- The Data Protection Act 2018 (including the relevant specific codes of practice e.g. Employment Practices)
- Records Management Code of Practice for Health & Social Care 2016
- Freedom of Information Act 2000 (FOI)
- The Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2000
- Children Act 2004
- Public Interest Disclosure Act 1998;
- Audit & Internal Control Act 1987;
- National Health Service Act 1977;
- Prevention of Terrorism (Temporary Provisions) Act 1989;
- Regulations under Health & Safety at Work Act 1974.
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998;
- Regulation of Investigatory Powers Act 2000
- Telecommunications Act 2000
- Police and Justice Acts 2006

Much of the relevant legislation is available on the following Internet link http://www.legislation.hmso.gov.uk/.

9. RELATED TRUST POLICY/PROCEDURES

- Network, Information Security and Risk Policy
- Freedom of Information Policy
- Removable Media Policy
- Records Management Policy
- Disciplinary Procedures Policy
- Equality and Diversity Policy
- Harassment at Work Policy

Equality Analysis

"St Helens and Knowsley Teaching Hospitals NHS Trust is committed to creating a culture that promotes equality and embraces diversity in all its functions as both an employer and a service provider. Our aim is to provide a safe environment, free from discrimination, and a place where all individuals are valued and are treated fairly. The Trust adheres to legal requirements and seeks to mainstream the principles of equality and diversity through all its policies, procedures and processes.

The Trust takes a zero tolerance approach to all forms of discrimination, harassment and victimisation and will make every effort to ensure that no patient or employee is disadvantaged, either directly or indirectly, on the basis that they possess any of the "protected characteristics" as defined by the Equality Act 2010. The protected characteristics are as follows: - race; disability; sex; religion or belief; sexual orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; and age.

This policy will be implemented with due regard to these commitments.

All authors of policy documents must include a completed equality analysis Stage 1 screening. Policy authors must refer to the Trust Equality and Diversity Policy and the equality analysis toolkit and associated guidance documents (Stage 1 and Stage 2) available on the intranet.

Equality Analysis for this policy

Equality Analysis Stage 1 Screening		
	Title of Policy:	Code of Confidentiality
	Policy Author(s):	IG Manager
	Lead Executive:	Director of IT
	Policy Sponsor	Director of IT
	Target Audience	All Staff
	Document Purpose:	This document is a guide to required practice and responsibility for those who work within or under contract to the Trust concerning confidentiality of staff and patient information and patients' consent to the use of their records.
	Please state how the policy is relevant to the Trusts general equality duties to: • eliminate discrimination • advance equality of opportunity • foster good relations	This document is the key guidance document to ensure the security and confidentiality of staff and patient information and supports the general equality duties.
	List key groups involved or to be involved in policy development (e.g. staff side reps, service users, partner agencies) and how these groups will be engaged	This policy is a revision. Consultation has been held with suitably qualified members of staff within the Trust who can advise on such topics. In addition the Policy was sent out for consultation on the staff intranet

	NB Having read the guidance notes provided when assessing the questions below you must consider;		
	• Be very conscious of any indirect or unintentional outcomes of a potentially discriminatory nature • Will the policy create any problems or barriers to any protected group? • Will any protected group be excluded because of the policy? • Will the policy have a negative impact on community relations? If in any doubt please consult with the Patient and Workforce Equality Lead		
	Does the policy **significantly** affect one group **less** or **more** favourably than another on the basis of: answer 'Yes/No' (please add any qualification or explanation to your answer particularly if you answer yes)		
		Yes/ No	**Comments/ Rationale**
	• Race/ethnicity	No	
	• Disability (includes Learning Disability, physical or mental disability and sensory impairment)	No	
	• Gender	No	
	• Religion/belief (including non-belief)	No	
	• Sexual orientation	No	
	• Age	No	
	• Gender reassignment	No	
	• Pregnancy and Maternity	No	
	• Marriage and Civil partnership	No	
	• Carer status	No	
	Will the policy affect the Human Rights of any of the above protected groups?	No	
	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	n/a	
	If you have identified a negative impact on any of the above-protected groups, can the impact be avoided or reduced by taking different action?	n/a	
	How will the effect of the policy be reviewed after implementation?	The policy will be audited at least annually in line with the key performance indicators	
	If you have entered yes in any of the above boxes you **must** contact the Patient and Workforce Equality Lead (ext. 7609/ Annette.craghill@sthk.nhs.uk) to discuss the outcome and ascertain whether a **Stage 2 Equality Analysis Assessment** must be completed.		
	Name of manager completing assessment: (must one of the authors)	Craig Walker	
	Job Title of Manager completing assessment	Director of Informatics	
	Date of Completion:	23.09.2014	

9. Training

All staff must attend mandatory training as per Trust Policy in order to comply with this policy.

10. Appendix

10.1. Appendix A: - Related Documents (Policies and Government legislation)

Users will be obliged to comply with legislation as appropriate including:

- Network, Information Security and Risk Policy
- Freedom of Information Policy
- Removable Media Policy
- Records Management Policy
- Disciplinary Procedures Policy
- Equality and Diversity Policy
- Harassment at Work Policy
- General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (including the relevant specific codes of practice e.g. Employment Practices)
- Freedom of Information Act 2000 (FOI)
- The Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2000
- Children Act 2004
- Public Interest Disclosure Act 1998;
- Audit & Internal Control Act 1987;
- National Health Service Act 1977;
- Prevention of Terrorism (Temporary Provisions) Act 1989;
- Regulations under Health & Safety at Work Act 1974.
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998;
- Regulation of Investigatory Powers Act 2000
- Telecommunications Act 2000
- Police and Just Acts 2006

Much of the relevant legislation is available on the following Internet link http://www.legislation.hmso.gov.uk/.

10.2. Appendix B – Full Responsibility Around E-mail And Internet Use.

10.2.1. Organisational Responsibilities

- Establish adverse incident and investigation procedures for the reporting of all breaches of this policy through the appropriate management channels
- Ensure that line managers understand their responsibilities for the implementation of this policy within their business or clinical area and that their managed staff adhere to the principles
- Provide appropriate training on the acceptable use of e-mail and the internet
- Ensure that controls are in place to prevent unauthorised access to the computer systems that allow access to the e-mail and internet system
- Compliance with section 46 of the Freedom of Information Act Code of Practice on Records Management with relation to disclosure of e-mails
- Defining acceptable personal use of e-mail and the internet

10.2.2. Caldicott Guardian Responsibilities

- Ensure that the organisation is aware of key legislation relating to this policy
- Ensure that systems are in place to investigate breaches of this policy
- Guide the organisation on the transfer or disclosure of person identifiable information by e-mail and the internet

10.2.3. Line Managers Responsibilities

Line Managers must ensure that permanent/temporary staff, students, trainees and contractors working in their departments are aware of:

- This policy and related policies
- The acceptable personal use of e-mail and the internet
- How to access advice and guidance on e-mail and internet acceptable use
- The security of the physical environment in their department
- How to report breaches or potential breaches of the E-mail and Internet Policy
- Line Managers can request monitoring of e-mail or internet use of their staff following the principles set out in section 5.4
- Line Managers must ensure they set the acceptable use standards for their staff.
- Once a Line Manager has been notified of a breach of this policy they should report the incident immediately to the Caldicott Guardian or Information Governance Manager via Datix, giving details of the breach, date, time, place and any other relevant information.
- Any inadequate procedures that might lead to a breach should also be reported by the process set out above.

10.2.4. Health Informatics Responsibilities

- Reviewing this policy in line with changes in legislation/guidance/standards
- Providing, managing, and maintaining the e-mail system and internet access
- Monitoring and auditing access (see section 5.4)
- Supporting the investigation of reported incidents
- Complying with legitimate requests for access to mailboxes (see section 5.4)
- Staff training on the acceptable use of e-mail and the internet
- Maintain the library of blocked URL categories.
- Username and password management
- Virus control
- Reporting incidents and inappropriate use to the Board through the information Governance Steering Group
- Reporting on issues raised
- Disseminating this policy in the organisation
- Acting as a source of help, advice and guidance on the acceptable/unacceptable use of e-mail and the internet and the content of this policy
- Ensure that all consultants, executives and suitably authorised individuals have access to streaming video and social networking sites to assist in the conduct of their duties.
- Responsible for monitoring as described in section 5.4.
- In order to ensure staff are abiding by policy the Trust will monitor all e-mails that are sent externally. Monitoring will be to ensure compliance with this policy and in particular will be looking for e- mails containing patient/ sensitive /personal identifiable information. Where necessary, the Trust will contact individuals who are sending such information out inappropriately.
- The Informatics Department will only initiate a request for access to an individual's mailbox or a restricted website, when a request for this access has been made in writing from the Service Director to the Assistant Director of ICT.
- The Informatics Department will only initiate a request for access to individual's internet records, when the Assistant Director of ICT has received a written request from the Service Director of the Trust area in question.

10.2.5. Information Security Officer

The Information Governance Manager will task the Information Security Officer with performing all monitoring actions and report upon findings to the IG Manager as and when required.

10.2.6. Staff Responsibilities

Staff must:

- Comply with this policy at all times including any use of the service whilst off duty
- Report any incidents such as inappropriate use or security breaches or virus infection to their line manager
- Complete the signatory document in Appendix D after reading this policy
- Always ask for advice and guidance on the content of this policy or use of e-mail and the internet from line managers or the Health Informatics Service Helpdesk if unsure of the content
- The Informatics Department has blocked certain inappropriate sites to prevent accidental access. Staff should not try to bypass security systems to try and access such sites.
- If a staff member accidentally accesses material of the type referred to in the previous paragraph or other material which may be considered offensive, they should note the time and web site address, exit from the site and then inform their line manager who will instigate the Trust's reporting procedures
- Staff must not sell or provide non-Trust products or services or otherwise conduct non-Trust business via Trust provided internet access
- If a staff member is in doubt as to whether it is appropriate for them to access a site, they should speak to their line manager before doing so.
- Only those staff who are specifically authorised to give media statements on behalf of the Trust may write or present views, concerning the Trust and its business, on the internet.
- Staff must never access the internet using another individual's login. It is totally unacceptable to adopt a colleague's identity on any internet site.
- Where an individual orders personal items from an internet site (for example, internet shopping) they must not arrange for them to be delivered to any Trust premises
- Staff must not download, upload, access or distribute any material whose subject matter is:
    a. Unlawful,
    b. Objectionable,
    c. Causes offence, - examples of which are material which is libellous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability this includes incitement of hatred or violence or any activity that contravenes the Law or the Trust Policies listed in Appendix A,
    d. Material that could be classed as abusive, indecent, obscene, menacing; or in breach of confidence, copyright, privacy or any other rights.

- Confidential information in relation to the business of the Trust and/or service user/another staff member's identifiable information must never be disclosed or placed on internet sites or chat rooms.
- Staff should inform the Helpdesk where any suspicion of virus infection arises.
- Staff must not download or distribute copyrighted material without permission of the copyright holder, this applies to any download for work or personal use.
- Staff should not download software onto Trust computers, including laptops.
- Staff should not store downloaded information for personal use on the Trust Network
- Staff should not connect to other networks (including peer-to-peer networking systems) to download files or software, unless authorized to do so by the Deputy Director of Informatics, usually in cases where the service is required to in order to fulfill its obligations.
- Staff who access or are members of social media sites in a private capacity must not post images that have been taken inside of, in the grounds of, or of Trust premises, or place misleading, malicious, or derogatory comments or references that would damage the reputation of, or misrepresent the Trust, or cause distress to its service users or any other member of staff.
- Staff must not use a Trust e-mail address to sign up to social media sites for personal use.
- When using social media for personal purposes, you must not state or imply that you are speaking on behalf of the Trust. If confusion is likely to arise, you may wish to use a disclaimer that clarifies things, for example 'these are my personal views and not those of my employer'.
- Staff must not disclose any confidential information relating to the business of the Trust, to their employment at the Trust, to the employment of colleagues or relating to any staff members.
- Staff must comply with all Trust policies when using social media. For example, you should be careful not to breach the Trust's Information Security Policy or Code of Confidentiality
- Sites must not be used to abuse other staff members, service users or volunteers. Privacy and feelings of others should be respected at all times.
- Staff must consider carefully whether it would be appropriate to befriend someone when using social media for personal purposes where there is a professional/client/pupil relationship, and/or where this could create a potential conflict of interest.
- Viewing and updating sites, blogs or other regular web presences used for purely personal purposes should not take place during working time (which excludes recognised breaks).
- If approached by a media contact about content on a site relating to the Trust, staff should immediately contact the Head of Media, PR and Communications for advice and support, following the existing policy.

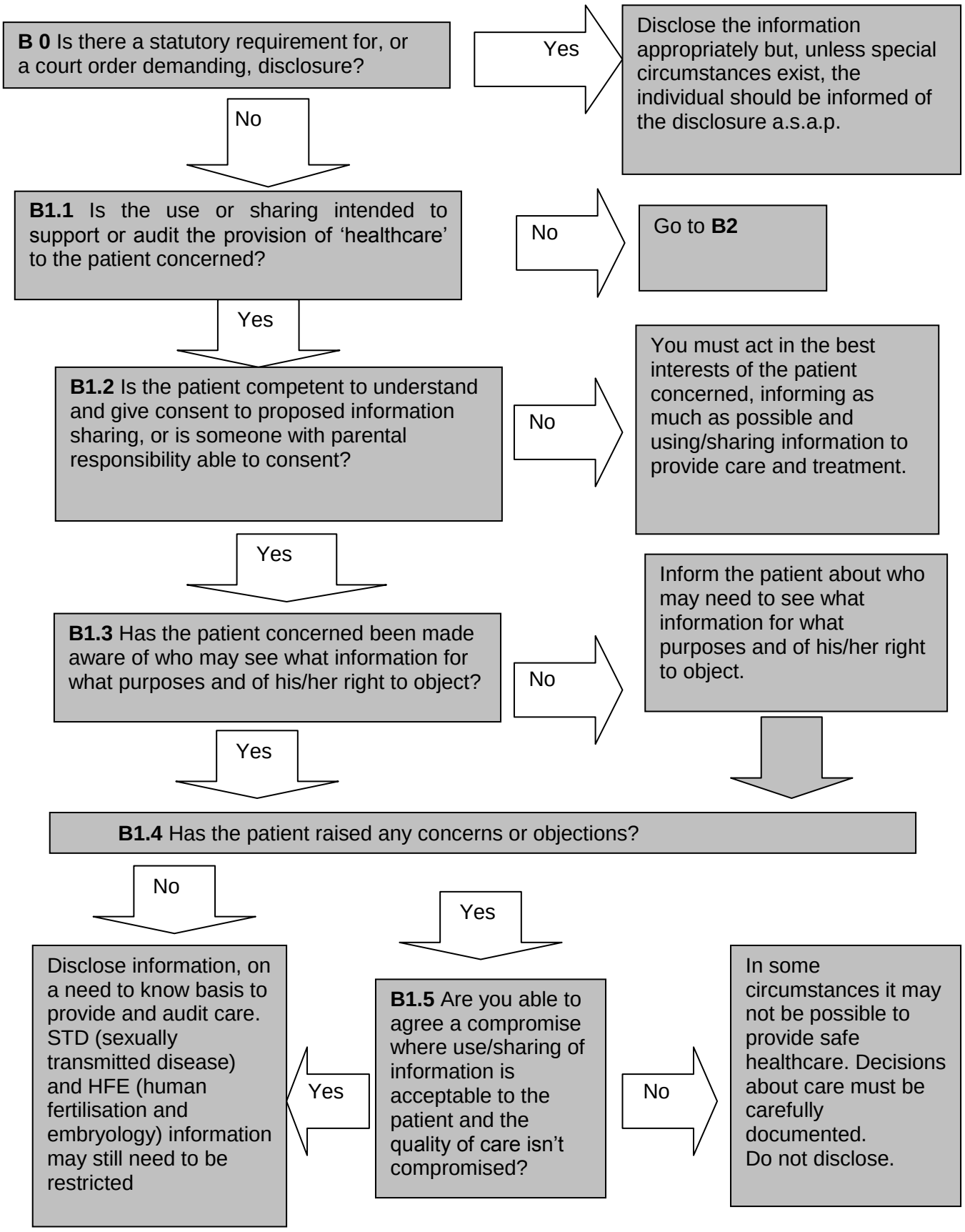
- Staff members should identify themselves as staff of the Trust only when appropriate.
- Staff must not share their password and user name with any other person and should not leave their computers unattended and unlocked whilst logged on, as they will be held responsible for any activity which takes place using their account.
- Unauthorised use of someone else's identity to send or intercept e-mail is strictly forbidden and will result in disciplinary action.
- Staff must not distribute any material by e-mail which is:
    a. Unlawful,
    b. Objectionable
    c. Causes offence, examples of which include but is not limited to offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability
    d. Contains material which is libellous or pornographic or includes incitement to commit a crime, hatred and violence or any activity that contravenes any of the Trust's Policies including Equal Opportunities Policy.
    e. Material that could be classed as abusive, indecent, obscene, menacing, or in breach of confidentiality, copyright, privacy or any other rights.
- Any member of staff who receives e-mail containing material which is in breach of this policy should inform their line manager immediately, who will institute the organisation's incident reporting procedures. Distribution of such material may result in legal action and/or disciplinary procedures.
- Where a member of staff receives e-mails from unsolicited sources, the sender should be added to the receiver's personal 'Blocked Sender List' (The Helpdesk can provide instructions on how to do this if required). The Informatics department will occasionally review staff personal Blocked Sender Lists with a view to blocking e-mail from prolific unsolicited sources.
- Staff who receive e-mail attachments, where there is any doubt about the origin, should contact the Help Desk for advice. Viruses can be spread through e-mail and opening suspect attachments may result in loss of data or damage to the Trust IT systems.
- Staff must not use the organisation's e-mail system to conduct any personal business enterprise.
- It is considered inappropriate to forward or create chain letters to other e-mail users either within the organisation or externally. If a user receives a chain letter they must inform their line manager who will instigate the organisation's reporting procedures. A chain letter is a letter which compels the receiver to forward the message to others, usually with the threat of adverse consequences if this is not done.
- Chain letters sometimes contain warnings about virus outbreaks; these are often hoaxes which should not be forwarded or acted upon. If users are unsure as to the legitimacy of an e-mail they should forward this to the Informatics Department for investigation.

- To avoid inappropriate content being circulated and breaching the principles of the Data Protection Act and the General Data Protection Regulation, users should not set their e- mail to “auto forward”.
- Staff must never send patient identifiable information to external e-mail addresses (which includes their personal e-mail address).
- Only those staff members who are specifically authorised to give media statements on behalf of the Trust, i.e. the Communications, PR and Media Department, may write or present views, concerning the Trust and its business, via e-mail.
- Staff must never send patient identifiable information to their personal e-mail address.
- If a user is unsure of any aspect of sending person identifiable information electronically, then guidance should be sought from the Helpdesk.
- Staff must follow the principles outlined in this policy on sending information securely.
- The use of unapproved non-corporate deployed Instant Messaging (IM) clients and connectivity is strictly prohibited.
- Staff may browse the internet or use e-mail within the boundaries of this policy for their own personal use prior to or after their normal working hours or during their lunch break as agreed with their line manager. This time period should not exceed 1 hour.
- Staff should be aware of their responsibility to report any breach or risk to the confidentiality of information that they become aware of.
- Staff should report breaches to their line manager and through the Trust Incident Reporting Procedures (Datix). If users feel that it would compromise their position they may report the breach (confidentially) directly to the Caldicott Guardian or Information Governance Manager.
- Any inadequate procedures that might lead to a breach should also be reported by the process set out above.

Users of the internet must be aware that each site they visit is recorded and logs of sites are regularly examined. Inappropriate usage may result in disciplinary proceedings. Information can be shared with the Local Counter Fraud Specialist and will be utilised in fraud investigations. A full security audit trail is maintained of records/sites accessed.

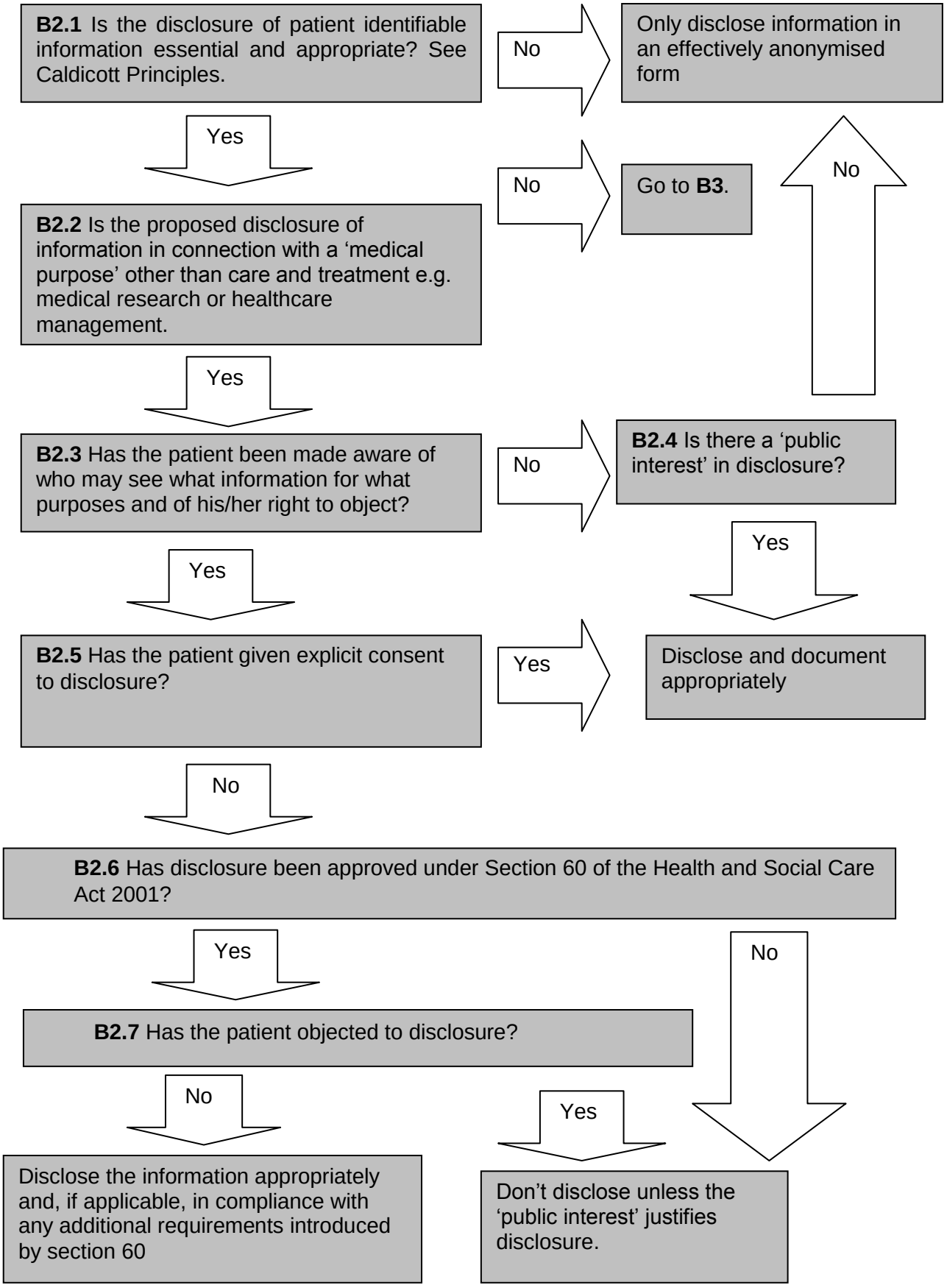
10.3. Appendix B1– Consent Sharing

Disclosure Model - where it is proposed to share confidential Information in order to provide healthcare



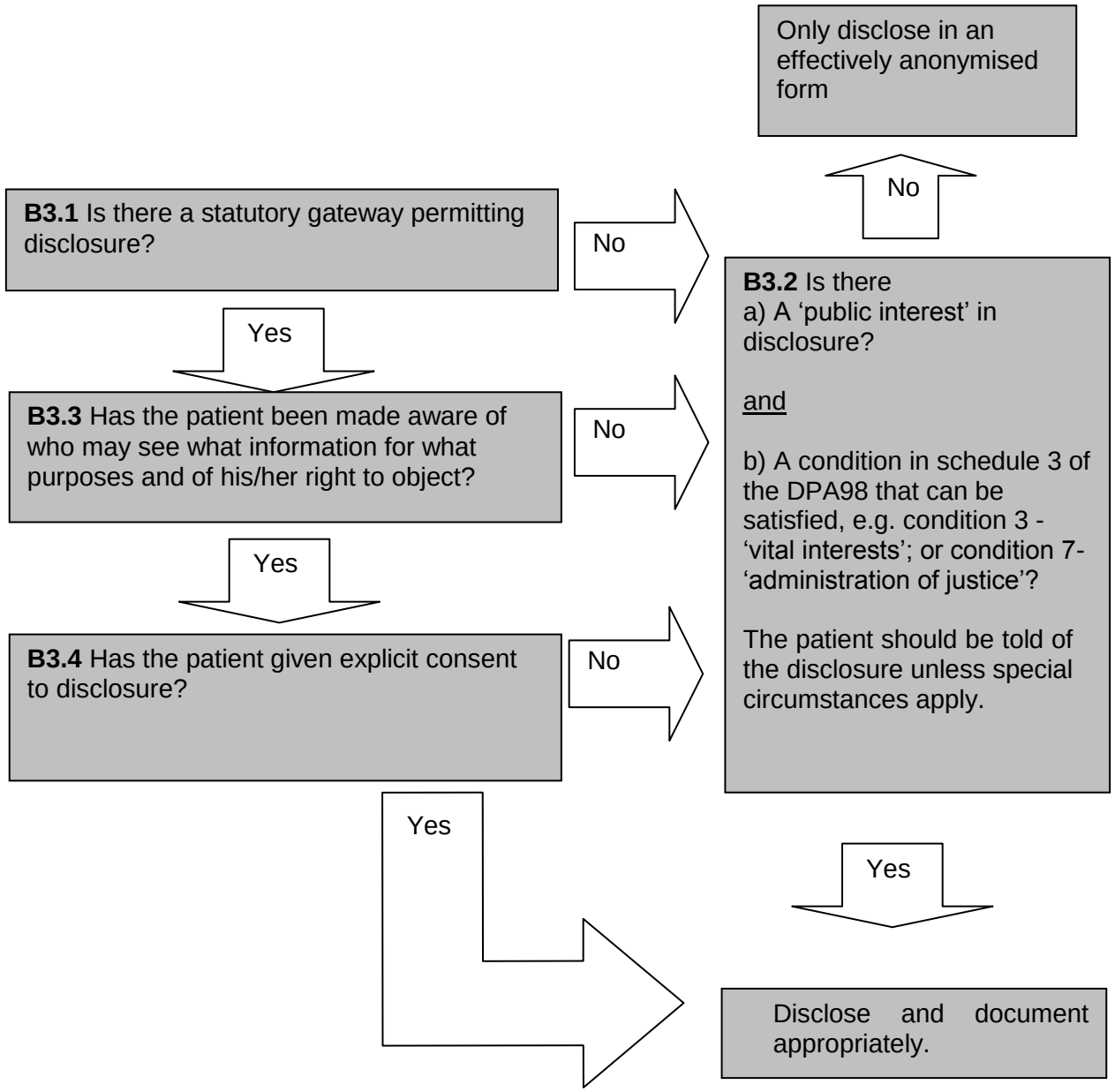
10.4. Appendix B2: – Consent Sharing

Disclosure Model - where the purpose isn't healthcare but it is a medical purpose as defined in the legislation



10.5. Appendix B3 – Information Sharing

Disclosure Model - where the purpose is unrelated to healthcare or another medical purpose



10.6. Appendix C

Legal Implications of E-mail and Internet

10.6.1. Email Legal Implications

E-mail has been established as a means of communication for businesses and its use is now widespread. E-mail carries the same legal status as written documents and should be used with the same care. Several factors combine to make e-mail a particularly important issue within Government legislation.

- Where an e-mail contains personal data it will fall within the boundaries of the Data Protection Act 2018 and GDPR.
- When e-mail content relates to a living individual its disclosure may be required under the data subject's rights under the Data Protection Act 2018 and GDPR.
- E-mails may be subject to disclosure under the Freedom of Information Act 2000.
- E-mails that contain inappropriate comments may constitute breaches of Equality and Diversity or Disability Discrimination, Human Rights or other similar legislation
- Sending emails that are offensive, abusive or harassing may constitute a criminal offence.
- E-mails are considered a form of publication and inappropriate comments may constitute libel contrary to the provisions of the Defamation Act 1996.

Misuse of e-mail and the internet may result in legal liability for the Trust and, in some cases, the individual user. Inappropriate use may give rise to

- Liability for defamation
- Copyright infringement
- Breach of confidentiality
- Inadvertently entering into contracts
- Claims of harassment and discrimination
- Claims for compensation

10.6.2. Social Media Legal Implications

All Trust staff should bear in mind that information they share through social media, even if they are on private spaces, is subject to copyright, The Data Protection Act 2018, The Safeguarding of Vulnerable Groups Act 2006, The Computer Misuse Act and any other relevant legislation.

Although individuals may believe they have restricted access of their profile to their "friend" list or list of contacts, the High Court has previously ruled that all postings to social network sites are regarded as being in the public domain and as such potentially accessible to all.

It is critical that staff comply with this policy in their use of social media sites. Failure to do so will lead to their conduct becoming subject to investigation under the relevant Disciplinary Procedure.

Staff should be aware that there is an implied legal duty of trust and confidence between an employer and employee. It is possible therefore that any inappropriate use of social media both in or outside the workplace, for example by making unjustified negative comments or defamatory comments about the Trust, its clients, or staff, could result in disciplinary action if it brings the Trust's reputation into disrepute, or exposes the Trust to potential liabilities. The Trust recognises and upholds the right of staff to make public interest disclosures ("whistleblowing"- See the Raising Concerns Policy) when necessary but would not envisage that such disclosures could be justifiably made using social media.

10.6.3. RIPA

The Regulation of Investigatory Powers Act 2000 (RIPA) & Telecommunications Act 2000

Section 1 (3) of RIPA prevents interception of communications in the UK without lawful authority. The Trust considers all the information that it holds to be valuable and will strive to ensure that it is therefore handled in accordance with Trust Policy. In order to ensure staff are abiding by policy the Trust will monitor all emails that are sent containing patient/ sensitive /personal identifiable information externally and where necessary contact individuals who are sending such information out inappropriately.

Under the provisions of the Act, the proposed monitoring of emails would amount to "interception of communications".
This interception of communications is rendered lawful as it is undertaken in compliance with the Telecommunications Regulations 2000. These Regulations talk in terms of "business practice" and business is defined as including activities of a public body such as the Trust. (Regulation 2a)

Regulation 3 of the Regulations permits the monitoring and recording of communications without consent to establish the existence of facts relevant to the organisation which can include:

- To ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business (such as compliance with the DPA regarding the disclosure of PID via email)
- To ascertain or demonstrate standards which are or ought to be achieved by staff using the system
- To Prevent or Detect Crime
- To investigate or detect the unauthorised use of the telecommunications system
- To ensure the effective operation of the system

To ensure the Trust is in compliance with the Telecommunications Regulations 2000, the Trust will have made all reasonable efforts to inform staff who may use email, that interception/monitoring of outbound emails, where personal data has been identified, will take place.

10.7. Appendix D: - Staff Signatory Page

IM&T Information Security
Code Of Confidentiality Acceptance Form

I have been given a copy of and have read and understood the Trust's Code of Confidentiality.

I understand that I must seek guidance from the Information Governance Manager or my Line Manager if any part of this policy is not clear to me.

I understand that, by accepting my account password and related information and accessing the organisation's Network and Internet system, I agree to adhere to this policy.

I understand that I must report any Network or Internet misuse to my Line Manager or Information Governance Manager.

I understand that I must follow the guidance in this document and must not breach any of the principles

I understand that if I let another person use my e-mail or Internet account I will be held equally responsible for any violations of this policy that may occur

I understand that if I breach any of the principles and guidance in this policy or fail to report violations of these principles by other users that I may be subject to disciplinary action.

I consent to the monitoring of my e-mail and internet use for the purposes of ensuring my compliance with the Code of Confidentiality.

Signed……...

Print name…….

Date……

This signatory document will be kept on your personnel record to appropriate records' retention periods

10.8. Appendix E: - E-mail Etiquette

- When sending messages or responding to messages sent by other users, your recipient might have different views, opinions and cultures. Without vocal inflection and body language, sarcasm, facetiousness and what you would consider innocent ‘fun’ can be misinterpreted as being rude or abusive.

- E-mail messages should not be written in CAPITAL letters as this is considered to be aggressive or the equivalent of shouting.

- The subject field should always be used to add a short description of the contents of the e-mail. This will assist the recipient in prioritising the opening of e-mail and will aid the retrieval of opened messages.

- Care should be taken with content. You should never write anything in an e-mail that you would not write in a letter or say to someone face to face. You should also take into account that e-mail records can be permanent.

- The same conventions should be used as when sending a letter by post, e.g. using the same style of greeting.

- E-mails should be signed off with the name, title and contact details of the sender. This can be added to a signature file so that it appears automatically (contact the Informatics Department for assistance with this if required).