Milton Keynes University Hospital NHS Foundation Trust

Policy	
Title: Information Governance Policy	
Classification :	Policy
Authors Name:	**Dawn Budd & Heidi Walker**
Authors Job Title:	**Information Governance Manager/Deputy**
Authors Division:	**Corporate**
Departments/ Group this Document applies to:	
Date of Approval:	**Review Date: May 2019**
Approval Group: TDC April 2018	**Last Review: May 2018**

Unique Identifier: ICT/GL/40	**Status:** Draft	**Version No: 5**
Policy to be followed by (target staff):		
To be read in conjunction with the following documents: Privacy notice IT policies Health Records policy Risk Management Strategy and policy Incident reporting policy		
CQC Fundamental standards: Regulation 17 – Good governance		

Index

1 Introduction 3
2 Scope 3
3 Information Governance Management 5
4 Roles and Responsibilities 6
5 Policy Definitions 8
6 Staff code of confidentiality 9
7 Data Protection Act 2018 including GDPR 10
8 Caldicott 11
9 Subject Access Request 12
10 Release of Personal Identifiable Information 14
11 Data Flow Mapping 18
13 Data Protection Impact Assessment (DPIA) 24
14 Information Asset Register 26
15 Third Party Agreements 28
16 Safe haven 29
17 Internet 32
18 Email 35
19 What's App 39
20 Risks to Devices 40
21 Text messaging 40
22 Photography, Video and Audio Recording 41
23 Smartcard Security 46
24 Mobile Computing 47
25 Copyright 48
26 Freedom of Information 52
27 Disposal 53
28 Retention of Records 54
29 Audits 54
30 Breaches of this Policy 55
31 Relevant acts of Law & Best Practice 55
32 Contact IG Team 58
Document review history 58
Consultation History 58
Audit and monitoring 59
Equality Impact Assessment 60

1 Introduction

Milton Keynes University Hospital NHS Foundation Trust (MKUHFT) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information Governance plays a key part in supporting Clinical Governance, service planning and performance management.
It also gives assurance to MKUHFT and to individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care and to meet the Trust's legal and good practice responsibilities.

The Data Security and Protection Toolkit covers: -

1. **Personal Confidential Data**
2. **Staff Responsibilities**
3. **Training**
4. **Managing Data Access**
5. **Process Reviews**
6. **Responding to Incidents**
7. **Continuity Planning**
8. **Unsupported Systems**
9. **IT Protection**
10. **Accountable Suppliers**

The Data Security and Protection toolkit provides a framework for handling personal information in a confidential and secure manner to the appropriate ethical and quality standards.
All initiatives of the Data Security and Protection Toolkit link together to: -

- Support the provision of high quality care by promoting the effective and appropriate use of information
- Encourage staff to work closely together, prevent duplication of effort and enable efficient use of resources
- Develop support arrangements and provide staff with the appropriate tools to enable them to discharge their responsibilities to a consistent high standard.
- Enable us to understand our own performance and manage improvement in a systematic and effective way.
- Enable us to audit patient information continually and ensure it is of high quality in accordance with both local and national information quality standards.

2 Scope

The scope of this policy is to establish and maintain the security, quality and confidentiality of information, information systems, applications and networks owned or held by the Trust by:

- Ensuring that all members of staff are aware of and fully compliant with the relevant legislation and sections in this policy.

- Describing the principles of security and explaining how they will be implemented within the Trust.

- Introducing a consistent approach to security and ensuring that all members of staff fully understand their own responsibilities
- Creating and maintaining a level of Information Security awareness within the Trust as an integral part of the day to day business.
- Protecting information assets under the control of the Trust.
- Assessing the training needs of staff against the Information Governance requirements and systems are in place and present within the organisational structure.

Objectives are to ensure:

Confidentiality	-	protecting sensitive information from unauthorised access or disclosure
Integrity	-	Safeguarding the accuracy and completeness of information and computer software
Availability	-	Ensuring information and vital services are available to users when required.
Quality	-	Ensuring information is of sufficient quality for the intended purpose
Transparency	-	Transparent in communication and exercising of the rights of the data subject

The potential impact of failure to preserve any of the above can have serious consequences not only for the Trust but also for our patients.

3 Information Governance Management

The Trust has appointed a Caldicott Guardian (CG) and a Senior Information Risk Owner (SIRO) to support the information Governance functions, both sit on the Information Governance Steering Group (IGSG) which has ultimate responsibility for the implementation of the Information Governance Agenda, this group reports directly to the Management and Trust Boards.

The operational management of Information Governance rests with the Trusts Director of Corporate Affairs.

The information governance steering groups responsibilities include: - (but are not limited to):

- Ensure the production of an Action Plan for the current year's assessment from the IG Toolkit.
- Ensure the production of an Audit Plan
- Recommendations for approval, by the appropriate Trust Board, related policies and procedures.
- Co-ordinate and monitor the Information Governance Strategy across the organisation.
- Appropriate policies and procedures are in place to underpin this function.

Principles of Information Governance

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

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 personal information about patients, staff and other Business Critical information.

The Trust recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the Data Protection Act 2018 including the General Data Protection Regulations (GDPR)

The Trust believes that accurate, timely and relevant information is essential to support high quality health care. As such it is the responsibility of all staff to ensure and promote the quality of our information.

Year on Year Improvement Plan and Assessment

An assessment of our compliance with requirements, within the Information Governance Toolkit (IGT), is undertaken each year. Annual reports and proposed action/development plans are presented to the Information Governance Steering Group. The yearly assessment is reported to Trust Board.

The annual assessment and action plan will inform the Trust Board of the current performance of the Trust and areas of concern to be addressed in the following year.

Training

The Trust will promote effective information governance practice to its entire staff through training. This will ensure that staffs are aware of their responsibilities in handling of and accessing information, irrespective of how that information is held.

All staff will attend, as part of their induction, a training session on Information Governance and refresher training must be undertaken via face to face training sessions, e learning or Information governance training booklets. Departmental training can be arranged through the Information Governance Team.

It is a mandatory requirement for all staff to attend Information Governance Training on an annual basis. Staff can book the session via the slate icon on their desktop.

4 Roles and Responsibilities

Caldicott Guardian / Deputy Caldicott Guardian

The Caldicott Guardian has a strategic role, developing security and confidentiality of patient information and to facilitate sharing where appropriate, and for representing confidentiality requirements and issues at Board level.

The Caldicott Guardian is the Trust's Medical Director who is responsible for agreeing and reviewing internal/external protocols governing the protection and use of patient-identifiable information.

The Caldicott Lead is the Information Governance Manager who is the first point of contact and undertakes all the duties above.

Senior Information Risk Owner/Deputy (SIRO)

The SIRO is a member of Trust Board who has lead responsibility to ensure organisational information risk is properly identified, managed and that appropriate mechanisms exist. The deputy SIRO chairs the Information Governance Steering Group and feeds up to the board.

Information Governance Manager

The Information Governance manager reports directly to the Corporate Services Director and is responsible for the Information Governance work program within the Trust. To include:-

- Investigating all Information Governance security breaches
- Acting as the Trust lead for Caldicott reporting directly to the Caldicott Guardian.
- Acting as the Trust lead for information risk reporting directly to the SIRO
- Ensuring that the Trust's business activities are conducted in a manner that is consistent with the Freedom of Information Act 2000, and that the Trust's activities consistently support accountability, openness, fairness and transparency of process.
- Approve all data flows for the release of personal identifiable information in conjunction with the Caldicott Guardian and SIRO.

Data Protection Officer

A data protection officer (DPO) is a leadership role required by the General Data Protection Regulations (GDPR). Data protection officers are responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements

The controller and the processor need to involve the DPO fully and at the earliest point in all issues which relate to the protection of personal data.

A consultative and Advisory Role to include the following: -

- Monitor Trust Compliance with GDPR
- Provide advice on DPIA's including the need to undertake one
- Investigate and report to the ICO all breaches within 72 hours (if a person's right is infringed)
- Undertake record keeping functions
- Independent and cannot be instructed to the output of advice

The IT Department

Where applicable the IT department will ensure that any technical requirements that are required to enact any part of this policy are fulfilled. This covers all Trust owned equipment and where applicable end user owned equipment being used to support the Trust business where this has been signed off and agreed.

Health Records Manager

The Trust's Health Records Manager will ensure that a systematic and planned approach to the management of health records is in place within the organisation via the Health Records Policy, which defines the requirements for the organization to control the quality, integrity and availability of information it generates, ensuring the organisation can maintain information in a manner that supports the safe delivery of patient care, and that it can dispose of the information appropriately when it is no longer required.

Operational and Line Management

Trust managers are responsible for ensuring that appropriate activities (training/user management) are facilitated for their staff and that compliance with this information governance policy is promoted.

All Staff

Staff members (full time and part-time employees of the Trust, non-Executive Directors, Contracted third party organisations and individuals including (agency, bank, locums, volunteers, student/trainees, and other staff on placement with the Trust,) are responsible for compliance with this Information governance policy.

Information Governance Steering Group (IGSG)

The Information Governance Steering Group's purpose is to drive the broader information governance agenda and provide the Trust Board with assurance that effective information

governance, records management and best practice mechanisms are in place within the organisation. The IGSG is also responsible for the monitoring and compliance of this policy.

Information Asset Owner IAO (System Owner)

Is a Senior Member of staff who is the nominated owner for one or more identified systems of the organisation. Information Asset Owners will support the organisations Information Governance goals and objectives by ensuring a system and its users comply with current legislation and to ensure the registration of the system is kept up to date and procedures are in place to achieve a high level of data quality.

Information Asset Administrator IAA

The Information Asset Administrator's (IAA) primary role is to support the IAO to fulfill their responsibilities. IAAs will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.

5 Policy Definitions

- Personal Identifiable data (PID) –is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context as defined in the Data Protection Act 2018 including GDPR.

- Special Category Data - is where the personal information contains details of that person's health or physical condition, biometrics, sexual life, ethnic origin, religious beliefs, trade union membership, political views, criminal convictions.

- Business Critical Information - where the loss of data would have a significant impact on the performance, reputation and operational effectiveness of the organisation. This may include but is not limited to Financial, personal, major projects.

- Healthcare Medical Purposes (Direct Healthcare) - which directly contribute to the care, and treatment of an individual or the Audit / Assurance of the quality of the healthcare provided

- Non-Healthcare Purposes (In-direct care) - Preventative medicine, medical research, financial audit, management of healthcare services, contract monitoring, and commissioning.

- Encryption - a process of scrambling data.

- Mobile Data Devices - For the purposes of this policy a mobile device is any device that can store digital information. This includes smart phones, tablet devices, notebooks and laptops. The device can be Trust owned or a staff owned device commonly referred to as a 'bring your own device' BYOD

- Bring Your Own Device (BYOD) - is a mobile device owned by an individual and used in part to access Trust data. The owner is responsible for the initial purchase of the device and any running costs that are incurred in its use. In addition the owner is entirely responsible for the on-going maintenance of the equipment and any personal data stored

on it.

- Virtual Private Network (VPN) - allows a user with appropriate authority to connect to the Trusts network from a remote location via the internet. The data is encrypted.

- Blogging - is using public website to write an on-line diary (known as a blog) sharing thoughts and opinions on various subjects.

- Electronic Data - is any data held in an electronic format

- Logical Concept - a set of rules, processes and behaviors' to which a small number of individuals are allocated

- Social Networking - is the use of interactive web based sites that mimic some of the interactions that occur between people in life. Examples include Facebook.com and Linkedin.com.

- Streaming: is the listening or watching of media without the need to download

- Section 251: Section 251 of the NHS Act 2006 relates to the disclosure and use of identifiable patient information in circumstances where patient consent has not been obtained, and, there is no other reliable basis in law to permit the disclosure and use of identifiable patient information

- Legitimate Relationship/LR: A connection to a patient that may justify access to the patient's personal data.

6 Staff code of confidentiality

Staffs need to be aware that:

They are individually responsible for the safekeeping of personally identifiable information on behalf of the Trust, when it is in their possession.

Everyone working for the Trust who records, handles, stores or comes across information that could identify a patient/staff member has a Common Law Duty of Confidence to that patient/staff member and the Trust.

Unlawful disclosure or misuse of personal data (including staff accessing their own personal staff or health records without authorisation or the records of colleagues, family or friends) is a breach of Trust policy and may constitute a criminal offence. All incidents of this nature will be fully investigated following the Trust disciplinary procedure and may be treated as a serious disciplinary offence and may lead to dismissal.

Everyone working for the Trust has a responsibility to comply with statutory acts that affect the processing and handling of information, confidentiality, the use of systems, and the protection of software.

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

Information should be considered confidential if it can be related in any way to a specific individual. The main areas of concern are any information that has not been fully anonymised. E.g. if name and address are not present but an NHS number is, this is not considered anonymous because it is still possible to trace that individual from the NHS number.

Confidential information will be found in a variety of formats including paper, computerised (including portable devices such as laptops and palmtops), visual and other versions of information storage media such as digital images and photographs. In addition, it covers oral communications including the use of the telephone (including mobiles) and general conversation.

The terms 'person-identifiable information' and 'person-identifiable data' are commonly used to mean any data item or combination of items by which a person's identity may be established. The main person-identifiable data items are:

Forename
Surname
Date of Birth
Sex
Address
Postcode
NHS Number, hospital Number or other patient numbers
Staff payroll number

7 Data Protection Act 2018 including GDPR

The Data Protection Act 2018 is the fundamental legal requirement that applies to all organisations and individuals processing data of a personal nature.
This Act applies to all personally identifiable information held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays etc.

The Act dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence and investigated in line with the Trust Disciplinary policy.

Data protection Principles

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the act in order to safeguard the rights and freedoms of individuals; and

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Rights of the Data Subject

- Right to be informed
- Right of access
- Right to rectification (Correction)
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Right to data portability
- Right to object
- Right to know if we carry out Automated indecision-making and profiling

If sending personal information outside the EEA ensure consent is obtained and the data is adequately protected.

8 Caldicott

The NHS best practice standard. The following principles underpin information governance across the health and social care services:

- Justify the purpose(s)
  Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

- Don't use personal confidential data unless it is absolutely necessary
  Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

- Use the minimum necessary personal confidential data
  Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

- Access to personal confidential data should be on a strict need-to-know basis. Only those individuals who need access to personal confidential data should have access. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

- Everyone with access to personal confidential data should be aware of their responsibilities. Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical staff are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- Understand and Comply with the law.

- Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Patients must be made aware that the information they give may be recorded and may be shared, In order to provide them with high quality care. It may also be used to support clinical audit and other work to monitor the quality of care provided.
Similarly, whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not always be the case and the efforts to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies.

In order to inform patients effectively, staff must:

- Ensure patients have received the Trust's patient information leaflet "A Guide to Patients on the use and storage of personal information". (Link)
- Make clear to patients the purpose of the health record and why and how the information is recorded. – See Privacy Notice (link)
- Make it clear to patients when they are or will be disclosing information to others and who these others may be.
- Check that patients are aware of the choices available to them in respect of how their information may be disclosed or used.
- Check that patients have no concerns or queries about how their information is disclosed and used. Where possible, answer any queries personally or direct the patient to the Information Governance Department.

9 Subject Access Request

Access to Health Records falls under the Data protection Act 2018 including GDPR and applies to records relating to the physical or mental health of an identifiable individual, which have been made by a Health Care Professional in connection with their care and treatment. This does not relate to the deceased which must be dealt with under the Access to Health Records Act 1990.

Rights of access

Patient Access

The right of access is principally for the individual who is the subject of the record, but the individual may authorise another person, to make an application for access on his or her behalf in writing. Other instances where an application to another person's record may be granted are:

- An Authorised person on behalf of the patient, i.e. relatives, or where an individual is incapable of managing his or her own affairs.
- Parents (The childs rights to confidentiality have to be balanced against parental responsibility).
- Patient representative – A person you nominate to make healthcare decisions
- Executor of a will/Persons who may have a claim arising out of the patients estate

Access to Medical Records by Patients, Solicitors/other third parties from an external source should be referred to the Information Governance Department on 01908 995042.

Access to medical records by other Hospitals and Healthcare organisations and other health professionals should be made to the Medical Records Department on 01908 995163.

In-Patient access to their medical records

Patients or relatives requiring access to the medical records whilst the patient is in hospital can be given as long as the following conditions are met:-

- There is no third party information within the record i.e. Social Services, Relatives, police etc.
- The records have been checked to ensure that there is nothing which will cause substantial harm or damage to the patient; these should be checked with the treating clinician.
- Access by a third party i.e. relative would need the patients consent, or legal basis.
- Parents of Children under the age of 13
- Parents of Children over the age of 13 if the child is not deemed responsible (Clinical decision/ Gillick Competent)

If read only access is required, the trust must ensure that a staff member is available to sit with the patient/relative whilst the record is accessed. This will ensure the record cannot be altered in any way

If a permanent copy is required this must be passed to the Access to Health Records Department to process.

Access which is required by all other bodies, i.e. Police, Social Services should be referred to the Information Governance Team, or the duty manager on call out of hours.

The Holder of the record

The Trust remains the legal holder of the record and has a duty to provide access to it after consultation with the appropriate Health Professional responsible for their care. The Information Governance Team will email the relevant Health Professional to inform them of the release of records for that patient. It is their responsibility to look over the records before disclosure to ensure that release of the record will not cause any substantial harm or damage.

All data must therefore be disclosed if a formal subject access request is made unless there is a danger of identifying a third party. In this situation the third party's consent must be sought and agreement had in writing before disclosure can occur.

The Trust must respond to subject access request within 1 calendar month

Employee Access to their Personnel Record

Requests from past or present employees for access to their personnel record will be directed to the Information Governance Manager who will be responsible for ensuring that appropriate identity checks are carried out and will then liaise with the Line Manager and Human Resources.

Fees

The Trust must provide a copy of the information free of charge. However, The Trust may charge a 'reasonable fee' if it receives requests for further copies of the same information, or refuse to respond when it a request is manifestly unfounded or excessive, particularly if it is repetitive.

Application for Access

Application for access to records under the Data Protection Act 2018 including GDPR must be made in writing via letter, email or the Trusts Application Form. The Trust has 1 calendar month from the receipt of a signed and fully completed application form to complete the request. Request forms can be obtained from the Trusts Intranet/Internet Access to Health Records Forms

10 Release of Personal Identifiable Information

This section addresses the risks of inappropriate or unlawful release of Person Identifiable Data (PID.

- Risks can occur when staff responds to ad hoc requests or where planned pieces for work or projects require the release of data. The risks can include:-
- Poor management of the methods of release and communication (e.g. failure to use encryption or secure transit)
- Not having a legal basis for the release of data e.g. the proposed use of the data is not the purpose for which it was originally collected
- Staff not having the authority to release the data or the recipient not being authorised to receive the data.
- Only staff that have been formally delegated the authority to release PID may do so.
- Staffs that have a Legitimate Relationship with patients need no additional authorisation to release information directly related to the treatment and care of individuals

Information Asset Owners will normally be authorised to release PID for which they are accountable, but where sensitive data or high volumes of data are concerned the authority of the SIRO or Caldicott Guardian and Information Governance Manager is required.

Transfers of PID outside of the UK must have authorisation from the Caldicott Guardian, SIRO and the Information Governance Manager.

Where Section 251 approval is thought to be required, Information Asset Owners should contact the Information Governance Manager.

Recording the releases of Ad Hoc Personal Identifiable Data

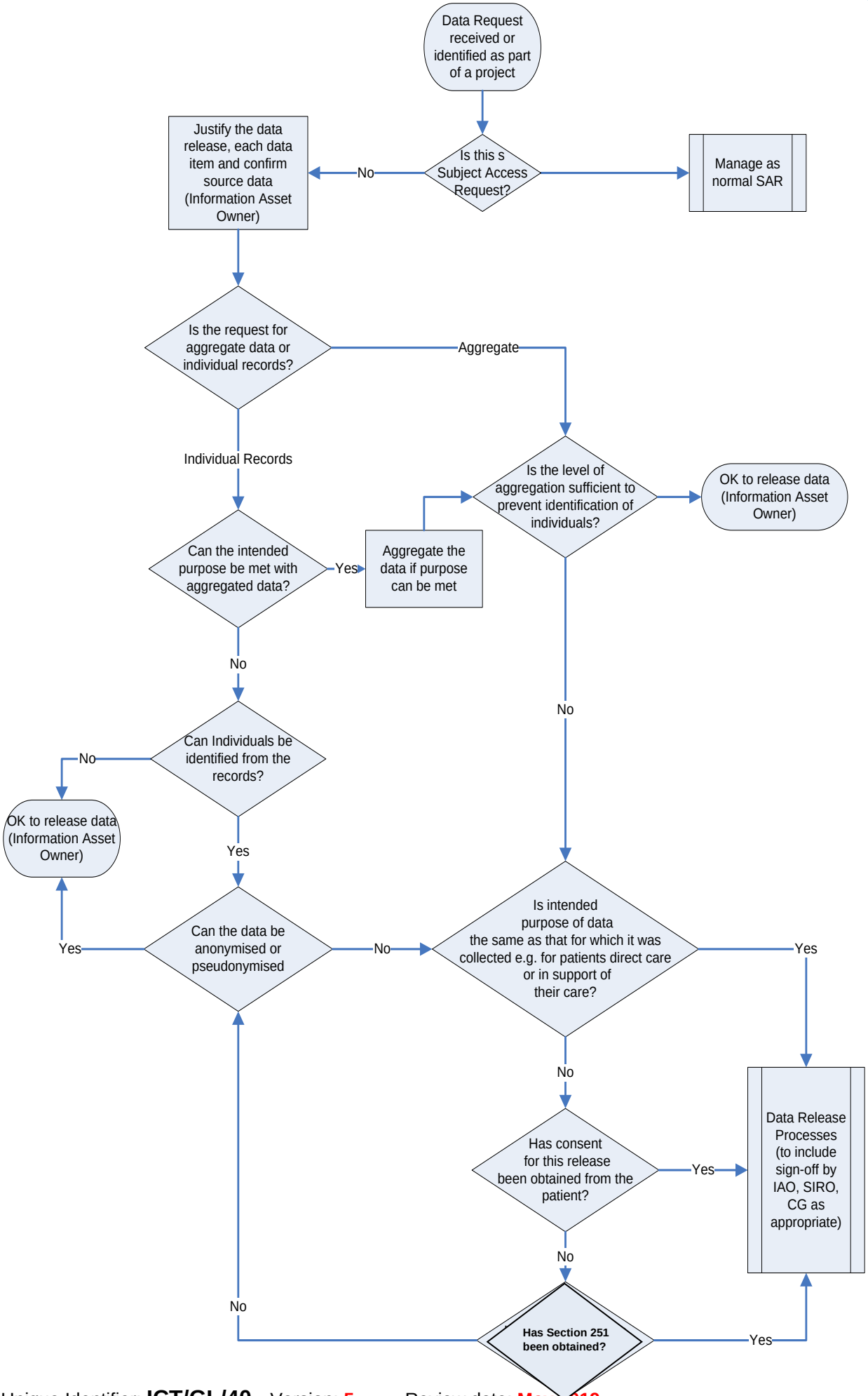
The Information Governance Team will maintain a Data Flow Register of all Trust ad-hoc releases of PID both in the UK and overseas. Ad-hoc Data Flows must also be added to departmental data flow mapping register if the flow is sent more than once.

A check list for all Ad-hoc data flows

The following is intended to provide a list of questions that should be answered when it is proposed to release any data that could potentially identify individuals and to ensure that any release is lawful. The checklist should be used in conjunction with the decision tree (Figure 1 below). Specialist advice on the questions and actions can be obtained from the Information Governance Team.

Ref	Action/ Questions	Comment	Suggested Action
	Justify the data release, each data item and confirm source data	Each data item should be justified. The period the data relates to and the purposes to which the released data will be put should be confirmed.	Discuss the requested data set with the proposed recipient. The data should be relevant and sufficient to meet the intended purpose and must not be excessive (i.e. include data not required for the purpose).
	Is this aggregate data or individual records?	Aggregated data will not usually allow the identification of individuals but this depends on the data items and the level of aggregation.	Where the intended purpose can be met with aggregate data, this is always preferable
	Is the level of aggregation sufficient to prevent identification of individuals?	For example, only a small number of individuals may live in a location defined by a full post-code and may be identifiable from the aggregate data. On average there are 15 addresses per full postcode with a maximum of 100 addresses. With staff data, small department size may allow individuals to be identified.	If not, consider different levels of aggregation e.g. use only the inward part of the code (the first part)

Ref	Action/ Questions	Comment	Suggested Action
	Can Individuals be identified from the records? Can the data be anonymised or pseudonymised?	Identifiers are: Direct identifiers - name, address Data used in combination - gender/ sex, date of birth, full postcode. For staff this could be department and grade. "Identifiers" - NHS number, Hospital number where the recipient has access to the associated demographic data. For staff these could be payroll number, NI number. Note that the data might be used in combination with other data that would then enable the identification of individuals.	Can the data be anonymised by removing identifiers or scrambling them? Can d.o.b be replaced by age? Can postcode be truncated? Can the identifiers be pseudonymised1?
	Has Section 251 been obtained?	Section 251 approval is needed in circumstances where patient consent has not been obtained, and there is no other reliable basis in law to permit the disclosure and use of identifiable patient information.	Identify organisational responsibility for doing this See guidance notes and application form
	Data Release Processes	See Section 11 above.	Involve Information Governance Manager / Caldicott Guardian or Senior Information Risk Officer Carry out risk assessment Ensure that contracts with the recipients of the data have adequate clauses covering IG, destruction of data Ensure media and communication of data are secure (e.g. encryption, use of NHSmail, Secure File Transfer etc.) Document and make appropriate register entry.
	Overseas Transfer		Ensure you complete the Data Flow form for sign off by the Information Governance Manager, SIRO or Caldicott Guardian Completed forms to be sent to the Information Governance Team for inclusion on the register



11 Data Flow Mapping

As part of The Data Protection Act 2018 including the GDPR
Organisations must map their data and information flows in order both into the organisation to assess their Privacy risks.

Understand the information flow

An information flow is a transfer of information from one location to another, for example:

- From department to department within the organisation.
- From The Trust to data external organisations, such as processors or suppliers

Describe the information flow and Identify key elements

Walk through the information lifecycle to identify unforeseen or unintended uses of data. This also helps to minimise what data is collected. Make sure the people who will be using the information is consulted on the practical implications and considers the potential future uses of the information collected, even if it is not immediately necessary.

Data items: *What kind of data is being processed (name, email, address, etc.) and what category does it fall into (health data, criminal records, location data, etc.)?*

Formats: *In what format do you store data (hardcopy, digital, database, bring your own device, mobile phones, etc.)?*

Transfer method: *How do you collect data (post, telephone, social media) and how do you share it internally (within your organisation) and externally (with third parties)?*

Location: *What locations are involved within the data flow (offices, the Cloud, third parties? Etc.)?*

Accountability: *Who is accountable for the personal data? Often this changes as the data moves throughout the organisation.*

Access: *Who has access to the data in question?*

Information Sharing

The following sets out the obligations and commitments that staff must follow to ensure that legislation is not breached, and patients'/ clients'/ service users'/ families'/ carers'/ staff/ employees' (collectively referred to as "individual") confidentiality is maintained. The Data Protection Act 2018/GDPR, The Computer Misuse Act 1990, The Common Law Duty of Confidence and Human Rights Act 1998 play a major role in the use and protection of personal identifiable information.

This section should be read in conjunction with the rest of this policy.

Information Sharing Principles

Sharing personal data is fundamental for the successful delivery and continuity of patient care.

Patient safety is paramount. If disclosure of confidential personal information is thought necessary in circumstances where, for example, a patient or other person is at serious risk from harm, and disclosure to an appropriate person would mitigate the risk, there is a legal right to breach confidentiality.

Consent to share will be sought from individuals who will be clear from the outset about why, what, how and with whom their personal information will, or could be shared, unless it is unsafe or inappropriate to do so.

Individuals must be confident that their personal information is stored safely and securely and that in the delivery of improved services and their privacy is not compromised.

Information sharing must be appropriate and proportionate for an organisation or practitioner to share information, it will be shared only with those organisations who need to have it, it will be necessary for the purpose that it is being shared, all decisions and reasons for sharing data will be recorded accurately.

- Information will be accurate and up to date; will be shared in a timely manner; will be shared securely; will be kept only as long as it is required and destroyed properly.
- Only the minimum information necessary for the purpose should be shared.
- When information needs to be shared, sharing complies with the law, guidance and best practice.
- Individuals' rights must be respected, particularly rights to confidentiality and security.
- Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure.

Wards and Departments should identify the circumstances when information is shared both on a regular basis and as a one-off. It is expected that any information sharing decision regarding a single individual at the point of care will be recorded in the clinical record. The details of the decision to share must be clearly recorded including whether consent has been obtained.

Considerations to be taken into account before information is shared:-

Are there any legal obligations to share information (for example a statutory requirement or a court order)?

The Trust must comply with Court Orders; however if there are concerns regarding the release of information to a third party, then arrangements can be made to release the information to the judge. The Information Governance team can provide guidance on a case by case basis

When patients give consent to disclosure of information about them you must make sure they understand what will be disclosed, the reasons for disclosure and the likely consequences therefore:-

- Explicit consent (must freely given)
- Be clear and concise.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.

The Trust will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.

The Trust recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest:-

- What is the sharing meant to achieve?
- Could the objective be achieved without sharing personal data?
- Is the sharing proportionate to the issue you are addressing?
- Only use confidential information when absolutely necessary.
- What do you need to tell people about the data sharing and how you will communicate that information?

Legal basis for sharing

Data processing is only lawful if the Trust has a legal basis for the particular processing activity taking place, so it may be lawful for the Trust to use a particular set of data for one purpose but unlawful to use that same data in a different context.

	Article 6 Lawful Processing
A	The data subject has given consent to the processing for one or more specific purposes
B	Processing is necessary for the performance of the contract with the data subject ; or to take steps to enter into a contract
C	Processing is necessary in order to protect the vital interests of the data subject or another natural person
E	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller includes processing of personal data that is necessary for : a) the administration of justice b) the exercise of a function in either Houses of Parliament c) the exercise of a function conferred on a person by an enactment, or d) the exercise of a function of the Crown., a Minister of the Crown or a government department
F	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

	Article 9 Conditions for Special Categories
A	The Data Subject has given explicit consent to the processing for one or more specific purposes
B	The processing is necessary for the purposes of exercising obligations or rights of the controller or data subject under employment, social security or social protection laws
C	Processing is necessary to protect the vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent
D	Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it about those purposes) and provided there is not disclosure to a third party without consent
E	Processing relates to personal data which are manifestly made public by the data subject
F	Processing is necessary for the establishment exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
G	Substantial Public Interest – A condition in this part of this Schedule is met only if, when the processing carried out, the controller has an appropriate policy document in place
H	This condition is met if the processing is necessary for health and social care purposes. "health or social care purposes" means : a) preventative or occupational medicine b) the assessment of the working capacity of an employee c) medical diagnoses d) the provision of health care or treatment e) the provision of social care, or f) the management of health care systems or services or social care systems or services
I	Public Health – This condition is met if the processing : a) is necessary for reasons of public interest in public health and b) is carried out _ i by or under the supervision of a health professional, or ii by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law
J	Archiving, Research and Statistics – this condition is met if the processing : a) is necessary for the archiving purposes, scientific or historical research purposes or statistical purposes b) is carried out in accordance with Aritic18991) of the GDPR (as supplemented by section 18), and c) is in the public interest

Patients who wish to opt-out of Sharing

In some circumstances patients may wish to opt-out of sharing their information for indirect care If a patient wishes to opt-out you should direct them to the NHS digital website to complete the national opt out form https://digital.nhs.uk/services/national-data-opt-out-programme

Patient Choice

Patients generally have the right to object to the use or disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment.

Children and Young People

Young people aged 16 or 17 are presumed to be competent for the purpose of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to make decisions about the use and disclosure of information they have provided in confidence.

However, where a competent young person or child is refusing treatment for a life threatening condition, the duty of care would require confidentiality to be breached (in the best interest of the patient) to the extent of informing those with parental responsibility for the child who might then be able to provide the necessary consent to the treatment.

In other cases, consent should be sought from a person with parental responsibility if such a person is available. It is important to check that persons have a proper authority (as parents or guardians).

Seeking and Recording Consent

Who is responsible for seeking consent for "Non Healthcare Purposes"?
Ideally, the senior health professional involved in the care of the patient should seek consent for non-healthcare purposes. The health professional should be supplied with all the necessary supporting information to appropriately inform the patient of the proposed use of their information and to answer any questions or queries arising.

Consent must be obtained prior to the information being used for other non-healthcare purposes.

To ensure that consent is appropriately sought the following should be applied:

- Explicit consent must freely given
- Be clear and concise.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.

The Trust will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.

Disclosure

Legally Required to Disclose

Some statutes place a strict requirement on clinicians or other staff to disclose information. Care should be taken however to only disclose the information required to comply with and fulfil the purpose of the law. If staffs have a reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the patient or another person, then they should seek legal advice. Consent of the patient or data subject is not always required but he/she should be informed preferably prior to disclosure, unless, informing the data subject is likely to place them or another person at risk.

Legally Permitted to Disclose

Legislation may also create a statutory gateway that allows information to be disclosed by an NHS body where previously it might have been unlawful to do so e.g. Section 115 of the Crime & Disorder Act 1998.

Disclosing (Sharing information with others) information with appropriate care
The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form except as originally understood by the confider, without his or her permission.

Legal Restrictions on Disclosure

There are two particular areas where there are legal restrictions on disclosing information and NHS organisations should take the necessary steps to secure any information capable of identifying an individual is not disclosed. These are:-

- Sexually Transmitted Diseases (STD)

Sexually transmitted diseases include HIV and AIDS. Information shall not be disclosed except:

- Where there is explicit consent
- For the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and for the purpose of such treatment or prevention.
- Human Fertilisation & Embryology

Identify enquirers, so that information is only shared with the right people.

Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information inappropriately. Seek official identification or check identity by calling them back (using an independent source for the phone number).

Check that they have a legitimate right to have access to that information and you have the right to disclose it.

Ensure that appropriate standards are applied for e-mails, faxes and post

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be, you should follow guidelines in this policy.

Share the minimum necessary to provide safe care or satisfy other purposes.

This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence. The Caldicott Principles should always be applied.

Safeguarding Children and Young People

The general principles of consent and confidentiality apply to situations involving safeguarding issues. There are areas which are more complicated, particularly over disclosure without consent and disclosure of information relating to family members rather than to the index case.

For further information on safeguarding please liaise with the safeguarding team and refer to Safeguarding Children Policy

13 Data Protection Impact Assessment (DPIA)

Data protection impact assessments (also known as privacy impact assessments or DPIAs) are tools which will help The Trust to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

DPIA's are structured risk assessments of the potential impact on privacy for a new or significantly changed process.

You should be aware that proposals that indicate a risk may still be adopted because it is possible that the risks can be mitigated or that the requirement is vital to the interests of the Trust making some risk acceptable.

DPIA's assist The Trust to:

- Anticipate and address the likely impacts
- Identify privacy risks to individuals
- Foresee problems
- Negotiate solutions
- Protect the Trust's reputation

When do you need to conduct a DPIA?

You **must** carry out a DPIA when:

- there are changes proposed to the way the Trust manages its person identifiable data or
- an introduction of a new system,

- Data Protection impact assessment (DPIA) needs to be completed before the change or installation.

Who should conduct a DPIA

If it has been confirmed that the project/change contains person identifiable information, it is the responsibility of the Project Manager (for new projects) or the Asset Owner to ensure that a DPIA is conducted and documented.

All DPIA's **must** be submitted to the Information Governance Steering Group, or if required urgently can be considered by the Trusts SIRO and ratified and recorded in the minutes of the Information Governance Steering Group at a subsequent date.

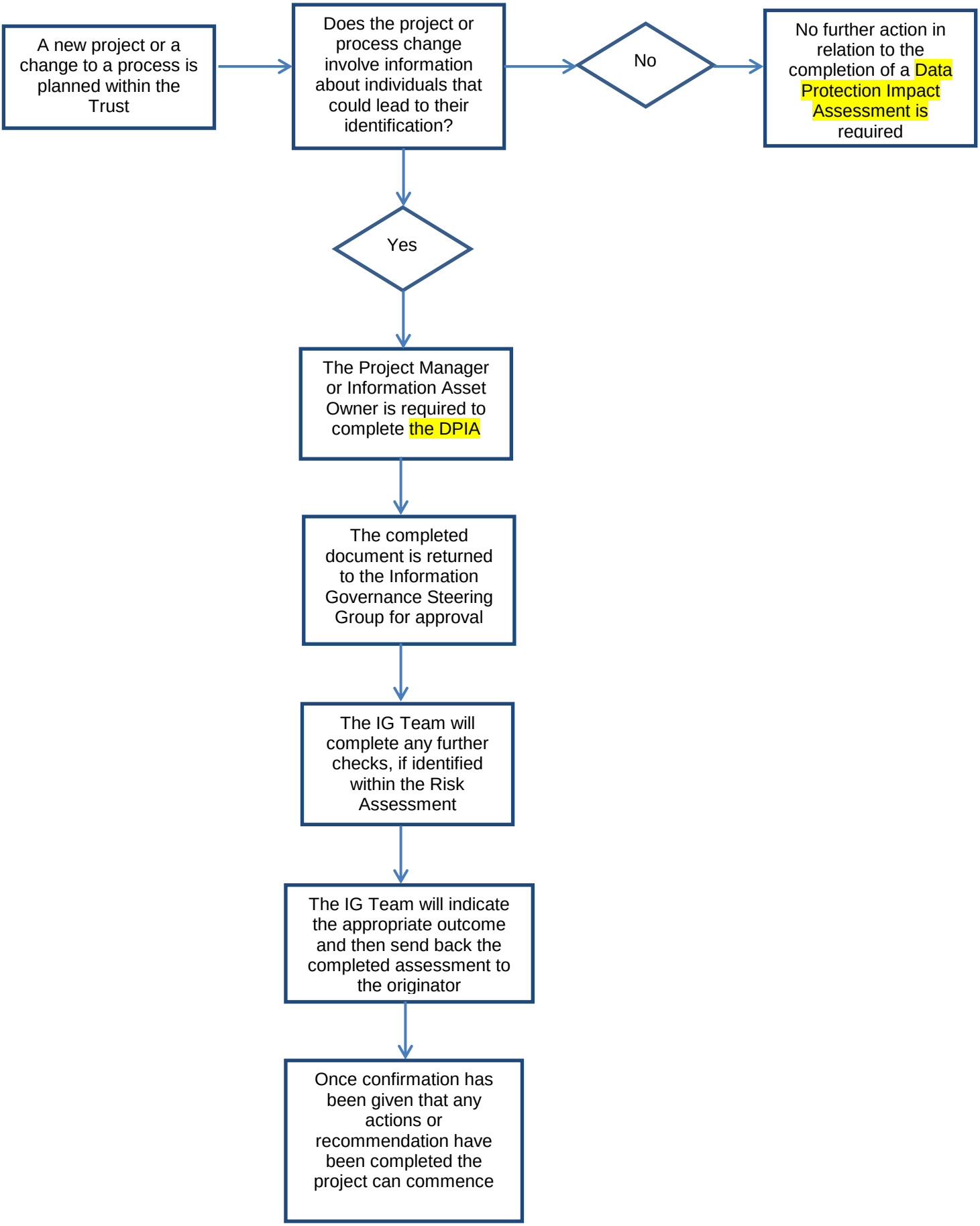
What information should the DPIA contain?

- A description of the processing and the purposes
- An assessment of the risks to individuals.
- The measures in place to address risk, including the security and to demonstrate that you comply the law.
- A DPIA can address more than one project.

Please note – A Data Protection Impact Assessment should only be considered if the system or process involved contains person identifiable information. If this is not the case then there is no requirement to undertake a DPIA at this time.

For all assessments please use the Data Protection Impact Assessment Template

Data Protection Impact Assessment Process Map



14 Information Asset Register

Departmental Information Asset Register

An Information Asset Register (IAR) is a simple way to help you understand and manage your Organisations information assets and the risks to them. It is important to know and fully Understand what information you hold in order to protect it and be able to exploit its potential.

Each department is responsible for creating an Information Asset Register for its key information.

What is an information asset?

An information asset is a single set of information (whether electronic or physical) that is held by, and is valuable to, the Trust.

This will include:-

- Documents that relates to the operational running of your department or the Trust and documents containing personal data – that is, information that can be used to identify a living person either directly or indirectly.

For example, a typical department might have information in some or all of the following categories:

- Databases or records about staff, patients, contractors or others
- HR files and folders which include personal data, for example job titles, grades, salaries
- Departmental health and safety records
- Audits undertaken by the department
- Project files
- Minutes of meetings
- Budgets
- Complaints

For further guidance and documentation please contact the Information Governance Department on 85044

Trust Systems Information Asset Register

A Trust wide system which holds and processes personal Identifiable data must have an Information Asset Owner. The owner must ensure that they have registered the system with the Information Governance Department and have the relevant documentation. I.e. Policy, third party agreements, business continuity plans, Training and guidance documents in place for that system and ensure they are kept accurate and up to date. .

15 Third Party Agreements

The Importance of robust Information Governance has risen rapidly in recent years following concerns about the security and confidentiality of Public Sector Data.

It is important that all Third Parties protect the Trust's information in line with Trust standards and Government Legislation.

All staff engaging a Third Party who may process information on behalf of the Trust must have obtained a signed agreement before commencement of the contract.

Third Parties are individuals and organisations outside of the Trust which fall into the following categories these will include, but not be limited to:

- Hardware and software maintenance and support staff
- Cleaning, catering, security guards and other outsourced support services
- Temps/agency staff
- Staff working within the Local Health Community
- External IT support staff
- Suppliers (including Suppliers of IT goods, systems or services)

It is important that all Third Parties protect the Trust's information in line with Trust standards and Government Legislation and therefore this must be adhered to when engaging Third Parties to maintain the confidentiality of our Personal Identifiable Data (PID) and Business Critical information.

A copy of the agreement can be found on the Trusts intranet site here

16 Safe haven

The Caldicott Report and more recently the Information Governance Toolkit has extended the concept of Safe Haven to all transfers of patient information and to ensure all routine inbound/outbound flows of patient-identifiable data both internally and externally are mapped.

Safe Haven comprises the facilities to restrict access by authorised users to identifiable data for the purpose of supporting de-identification, which in turn means that:

- The facilities can only be used by a small number of authorised staff sufficient to perform the functions and provide cover and back-up to ensure continuity of service.
- Authorisation of the staff performing the roles in the New Safe Haven should be through the Caldicott Guardian and the equivalent of local Registration Authority processes for accessing Spine based application.
- The systems (or sub-systems) used for the data transition processes must have appropriate access control mechanisms to restrict access to authorised users for specific purpose of supporting de-identification processes.
- The Safe haven may have a physical location, but it is only essential in the case of relevant paper based data flows, such as faxes.
- Safe haven can also be defined in terms of access control and data management arrangements as these indicate which data can be accessed by what means and by whom.
- Where Trust staff want to send personal information to other Trust locations or other agencies they should be confident that it is being sent to a location which ensures the security of that data.

Physical Security

- This could be a room that is locked or accessible via swipe access or a coded key pad known only to authorised personnel ;
- The office or workspace 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 any member of staff who work in the same building or office, or any visitors ;
- Manual paper records containing personal identifiable information should be stored in locked cabinets where possible ;
- Clear desk policy wherever possible should be in use ;

Fax Machines

The Trust is committed to reducing the use of faxes as this is not a secure method of transfer. It is important that information sent by fax is secure. Please refer to the Trusts basic rules for secure working leaflet. Discharge Summaries can no longer be sent by fax.

Communication by post

Information sent by post should be addressed correctly.

Communication by Telephone
Information should not be given out over the Telephone unless staffs is sure that the person requesting the information is who they say they are and that they have a right to receive the information. Please refer to the Trusts guidance leaflet on Telephone communication here

Electronic Systems
Access to any PC/system must be password protected. Staff must not allow others to access the Trusts systems under their user ID or share their password. Please refer to the Trusts guidance leaflet on passwords here

Access to systems will be given on a need to know basis and in line with the employee's job role.

Personal Information displayed on a PC monitor must not be left unattended.
The default timeout period before the PC automatically locks will be 10 or 15 minutes depending on the user.
To lock a computer - press ctrl-alt-delete.
Information should be held on the organisation's network servers, not stored on your desktop or local hard drives. Staff should be aware of the high risk of storing information locally and take appropriate security measures.

Staff are reminded it is essential that they log out of clinical systems once their session has finished, taking extra care using the computers on wheels (WOW). Leaving computer screen open containing confidential information is an information security breach and renders your access open to abuse. This could result in disciplinary action.

Great care should be taken in sending personal information especially where the information may be of a clinical nature – it should be encrypted and procedures undertaken to ensure that the correct person has received it. Please refer to the Email section within this policy

When using Registration Authority Smartcards staff must ensure they abide by the terms and conditions of use, please refer to the NHS digital guidance here

Group/Individual Job Role (Logical Concept)

This refers to a group of staff or individuals who are non-clinical that are perceived as safe havens due to the job role they perform and can view patient identifiable information i.e.

- Medical Records
- IT to include Back Office
- Access to Health
- Finance
- Data Quality
- Information
- Patient Experience
- Information Governance

- General Office
- Litigation Office

Verbal Communication

Requests for patient identifiable information must be verified to confirm the requester, are who they say they are and that they have a right to receive the information.

Where possible the staff member should ring the requester on the telephone number we have on record or by ringing the organisations switchboard and asking for that person.

If information is requested by the Police staff should direct them to the Information Governance Team during normal working hours or Manager on Call out of hours.

If contacting the patient directly it is important that staff make sure they are talking to the right person. It is not good practice to leave messages with others unless you have patient consent to do so.

Messages left on an answer phone should state name and telephone number of whom to contact i.e. Fred Smith 660033 ext. 6754, no personal identifiable information should be disclosed

Sharing Information with other Organisations (non NHS)

Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek an assurance that these organisations have a designated safe haven point for receiving personal information and that they have completed the Trusts third party policy.

The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirement:-

- Data Protection Act 2018/GDPR
- Common Law Duty of Confidence
- Privacy and Electronic Communication Regulations

Staff sharing personal information with other agencies should ensure that all Data Flow mapping has been logged on the departmental mapping tool.

17 Internet

The internet facility is provided by the Trust to support the Trust's goals and objectives.

Business Use

The primary use of the internet is for business purposes for which the user is employed; therefore any misuse of the internet facility will be investigated. There should be no expectation of privacy. Systems in place for monitoring purposes do not differentiate between business and private use.

The Internet is to be used in a manner, which is consistent with the Trust's mission and standards of business conduct. Usage of the Internet should be such that it does not diminish the Trust's reputation or indicate a lack of professionalism.

Personal Use

Limited personal use of Internet facilities is permitted provided the material accessed is appropriate and is not potentially offensive to others.

The use of the Internet for personal transactions only, such as booking reservations or tickets or the purchase of any goods or services for personal use, is permitted. Employees should regard this facility as a privilege that should be exercised in their own time without detriment to the job and not abused.

Access to websites that contain inappropriate material is strictly forbidden including pornography, instruction on criminal or terrorist skills, incitement to racial hatred, promotion of cults, gambling, content or statements of a nature which are liable to cause offence to others, or any other material likely to bring the Trust into disrepute.

Employees should operate the "Back" button immediately should they inadvertently access unsuitable material. Downloading of such material shall be deemed an act of gross misconduct. However, the Trust notes that access to subjects and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances, for example Sex education, youth advice, counselling on gambling, approved research. The Trust therefore places special responsibilities of care on staff operating in such areas to ensure that such access is necessary and that other users, staff and members of the community are not exposed to any such material without good cause.

Internet must not be used for the purpose of advertising, gambling or soliciting for personal gain or profit, not for the use of passing indecent, subversive or criminal data across or out from the organisation which may cause harm whether to an individual, groups or the organisation.

Staff must not use the internet for purposes of harassment or bullying.

The Internet access facilities may not be used to intercept information meant for others or to circumvent the access controls of systems and networks of other individuals or Trust's.

Files must not be downloaded from the Internet and used in such a way as to violate copyright and intellectual property right laws. Even if downloading is permissible under copyright law, there may be restrictions with regard to copying, forwarding or otherwise distributing files. Software license agreements should be read and adhered to. Staff must not transmit software, copyright or otherwise, from their computer via the Internet please see Copyright Section

Staff must not:

- Create or transmit "junk-mail" or "spam", including unsolicited commercial webmail, chain letters and advertisements.
- Create, download or transmit data or material that is created for the purpose of corrupting or destroying other user's data or hardware.
- Download or stream video or audio material for entertainment purposes.
- Use the Internet to conduct personal transactions neither in pursuit of their own commercial or business interests nor in such a way as to implicate the Trust in those transactions. If in doubt, staff should contact the Information Governance Team.
- Send information which is sensitive to the Trust's or its patients/staff, via the Internet, see Email section Email. All information sent to, or via, the Internet must be decent, legal and not disrespectful of the race, colour, creed or culture of others.

Unauthorised Disclosure of business critical or Personal Identifiable data

Blogging and social networking sites provide an easy means for information to leak from an organisation, either maliciously or otherwise. Once loaded to a site, organisational information enters the public domain and may be processed and stored anywhere globally. In short, organisational control is lost and reputation damage can occur.

Malicious attack associated with identity theft

People often place a large amount of personal information on social networking sites, including details about their nationality, ethnic origin, religion, addresses, date of birth, telephone contact numbers and interests. This information may be of use to criminals who are seeking to steal identities or who may sue the information for social engineering purposes

Legal liabilities from defamatory postings by employees

When a user registers with a site they typically have to indicate their acceptance of the site's terms and conditions. These can be several pages long and contain difficult to read legal language. Such terms and conditions may give the site "ownership" and "third party" disclosure rights over content placed on the site, and could create possible liabilities for organisations that allow their employees to use them. For example, where a user is registering on a site from a PC within the organisation, it may be assumed that the use is acting on behalf of the organisation and any libellous or derogatory comments may result in legal action. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.

Reputational damage

Ill-considered or unjustified comments left on sites may adversely affect public opinion toward an individual or organisation. This can lead to a change in social or business status with a danger of consequential impacts. Intimidation of employees from inappropriate use of sites will lead to investigations.

Software

Software downloaded from the Internet may cause virus infections and consequential damage. It may not be used on Trust's (or its clients) systems or data without the authorisation of IT. Additionally the client must also give their authorisation if their systems or data is involved.

www Sites

The creations of Web sites which indicate the involvement of the Trust (no matter how small) need the written approval of the Trust Chief Executive before they are created.

Monitoring

Inappropriate or excessive use of the internet may result in disciplinary action and/or removal of facilities. Staff should be aware that Internet access will be subject to monitoring and staff members informed if excessive use is noted. Any staff members actions deemed inappropriate will be reported to their line manager and investigated.

Anyone who is found to be regularly accessing, or on any occasion downloading illegal or indecent material may be summarily dismissed following procedures outlined in the Trust disciplinary procedure.

18 Email

The primary use of the email system is for business purposes for which the user is employed; therefore any suspected misuse of the system will be investigated by the Trust. There should be no expectation of personal privacy by the user if misuse is suspected.

E-Mail should be used in a manner that is consistent with the organisations mission and standards of business conduct. It should not diminish the organisations reputation nor indicate a lack of professionalism.

Use of the Trusts Internal Email System

E-mail is to be used for the purposes of the organisation to enable information to be passed across the organisation or from one organisation to another. E-mail should be viewed with the same status as any letter or memorandum and must meet the standards of business etiquette.

Personal use i.e. during staff lunch periods/breaks will be permitted provided that the content of the message is appropriate, and not likely to cause offence. It is strictly forbidden to include any form of pornography, instruction on criminal or terrorist skills, incitement to racial hatred, promotion of cults, gambling, content or statements of a nature which are liable to cause offence to others, or any other material likely to bring the Trust into disrepute.

Staff should regard this facility as a privilege which must be used in their own time without detriment to the job and not abused.

Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. Staff should be aware that both private and business use of e-mail may be subject to monitoring, and therefore there should be no expectation of privacy. Systems in place for monitoring purposes do not differentiate between business and private use.

Information included in any E-mails should be considered carefully, and staff should be aware that it is an official communication and as such can be stored and recalled for evidence.

Information contained in e-mails maybe subject to public disclosure under the NHS Code of Openness or the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure the confidentiality of e-mails and replies cannot be guaranteed.

Formation of Contracts - E-mail is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of employees inadvertently forming contracts on behalf of the Trust or varying contractual terms to which the Trust then becomes bound. Employees should take due care when drafting the words of an e-mail so that they cannot be construed as forming or varying a contract when this is not the intention.

E-mail must not be used for the purpose of advertising, gambling or soliciting for personal gain or profit, nor for the use of passing indecent, subversive or criminal data across or out from the organisation which may cause harm whether to an individual, groups or the organisation.

Staffs are actively discouraged in the use of attachments on E-mail messages as this increases risk of virus transmission. Viruses can only be passed on attachments when using E-mail. Should a virus be found then contact the IT Service Desk on ext. 87000

E-mails should not be deleted from systems deliberately in an attempt to destroy evidence. All staff is responsible for ensuring that any emails that need to be kept will be archived into their personal drives until the Trust secures an archiving facility.

Internal emails may contain personal Identifiable Information but this must be kept to a minimum e.g. NHS number or MRN number coupled with DOB for further ID identification.
This is subject to the normal rules of confidentiality and need to know basis.

Patient identifiable information MUST NOT be sent outside the Trust via mkuh.nhs.uk unless the Trust encryption facility is used alongside, alternatively this can be sent by NHS mail, please see guidance below. All flows of personal identifiable data must be logged on your departmental data flow mapping tool/chart. Emails may be monitored to ensure these guidelines are being followed.

Data, which is highly sensitive to the organisation or the client, MUST NOT be sent over the email except in exceptional circumstances and only following the approval of the Caldicott Guardian/Information Governance Manager.

Users must not:-

- Use the email management system to circumvent standard network and /or system access, through bypassing standard security controls or devices, or system audit functionality.
- Disguise their identity with intent to misrepresent any aspect of a communication
- Purposely disable or overload the email management system or network
- Purposely introduce computer viruses through email messages or attachments
- Forward chain emails or other frivolous material
- Use the email management system to violate the laws and regulations of the United Kingdom
- Send email communications persistently when, as a result of a complaint, a warning has been issued that further communications are not wanted.
- To avoid patient/person identifiable information being automatically sent to an insecure email address auto forwarding from a Trust email address to an external email is not permitted and therefore is automatically blocked and enforced centrally.

Use of NHSmail (www.nhs.net)

NHSmail is the email and directory service designed specifically for NHS staff and can be accessed via www.nhs.net it is the only BMA and Department of Health approved email service for

securely exchanging clinical data between NHS organisations but needs to be used by both sender and recipient.

Nhs.net to Nhs.net email addresses are encrypted.

Nhs.uk to Nhs.net email addresses are **NOT** encrypted

If you need to use this system for the secure transfer of data you will need to set up your own account directly on their website (www.nhs.net) or contact the IT service desk on 01908 997000 (87000).
Please ensure that you abide by the NHSmail policies and procedures.

If the Trusts email system is used to send patient identifiable/business critical information and you have the authority to do so, content encryption is available and must be used when emailing outside of the organisation to a third party.

To encrypt your email please type **(encrypt)** within the body of the email, this will trigger an email from the Trusts encryption service and you will receive a password for the recipient.
Do not email the password to the recipient

For all other communication please continue to use Milton Keynes University Hospital NHS email system.

Email sent to the communities below will be securely routed by NHSmail over the Government Secure Intranet (GSi) if they are sent to the specified formally accredited secure email services. Content does not need to be encrypted.

Secure email domains in Central Government:

*.gsi.gov.uk Until March 2019	*.gse.gov.uk Until March 2019	*.gsx.gov.uk Until March 2019

The Police National Network/Criminal Justice Services secure email domains:

*.police.uk	*.pnn.police.uk	*.scn.gov.uk	*.cjsm.net

Secure email domains in Local Government/Social Services:

*.gcsx.gov.uk Until March 2019

.

Breaches

Email and its usage will be monitored closely by the organisation; any misuse of the system will be reported to your line manager. In cases where inappropriate usage of email occurs an

investigation will be undertaken. This investigation may result in the confiscation of the individual's machine to confirm suspicions.

Formal disciplinary action may be taken up with any individual who uses email in appropriately.

E-Mail Housekeeping

The User should

- Log in at least twice a day and respond to requests promptly
- Advise people when you are not available. Use the out of office function.
- Be selective about who receives your e-mails particularly when using "Reply to all". Do all recipients need to see your reply?
- Use distribution lists with care. Do all recipients need to see this information?
- Use organisation wide distribution lists only to communicate important business information that has a genuine site wide value.
- Check that e-mails are addressed to the correct recipient, particularly if e-mailing to an external source.
- Check the e-mail before sending. Once you have clicked the send button you cannot stop it.
- Print only essential messages
- Use forwarding/reply with caution.

The holding of superfluous material introduces additional costs in storage and maintenance and can create a confusing work environment. Email boxes should have regular housekeeping checks to ensure data is managed effectively to enable the facility to run smoothly.

E-Mail Etiquette

- Sign off with your name, organisation and telephone number
- Use the subject field with a few short descriptive words to indicate the contents when sending e-mails. This will assist the recipient in prioritising and aids future retrieval.
- Type your message in lower case. Using capital letters can be considered aggressive.
- Be careful about the content; make sure it adheres to this policy.
- Maintain the conventions normally used in sending a letter by post. If you usually address someone as "Dr Smith", do the same in e-mail. E-mail carries the same etiquette as traditional communication; they also carry the authority of the sender!

19 What's App

WhatsApp is a free messaging application available for smartphones. WhatsApp uses your phone's Internet connection or Wi-Fi as available to let you message individuals, or groups. Following interest in WhatsApp for corporate use within the Milton Keynes University NHS Trust the following guidelines must be adhered to.

Users

WhatsApp can now be used within the Trust and externally outside to communicate with both colleagues and patients. This is considered more secure as the messages are now encrypted end to end. As with any system you need to be conscious of its use and ensure that you have the right security measures around your device as follows:-

- Always make sure that your device has a passcode on
- Lock your device when not it use (automatic lock)
- Be aware that this application can make use of your contact lists.

Use for Patient contact

If you choose to use this application to contact patients the following rules must be adhered to:-

- Do not record patient telephone numbers in your contact list (WhatsApp can use your contact list unless you opt out of this facility).
- Whilst communicating with patients this must be via a work phone, **under no circumstances** must you message more than one patient at a time.
- Use minimal data, i.e. surname, MRN and location.
- Use patient contact details and address only which is given to you by the patient and ensure permission is obtained to use this media before use.
- Images must not be taken using this media (the Trust is looking at this under separate cover).

Use between clinician/Clinical Groups

What's App can be used within the hospital setting between colleagues, the following rules must be adhered to:-

- Use minimal Identifiers i.e. surname MRN and location
- Ensure appropriate device security such as passwords
- Images must not be taken using this media (the Trust is looking at this under separate cover).

Housekeeping

It is important to remember that information has a shelf life and individuals should not be storing data which is no longer needed nor has any clinical or commercial value. Users must ensure:-

- Clear chat messages at the end of each month or sooner if no longer required
- Information within chat which has a clinical need to be kept must be transferred to the medical record and then deleted.
- Do not export chat or archive.

20 Risks to Devices

The listing below identifies the risks the Trust may be subjected to:

- All Trust PC's are at a potential risk from theft and therefore device encryption has been installed on all PCs across the organisation to ensure the security of patient identifiable data (PID) and business critical information and to protect against unauthorised access/loss.
  You must not save any personal identifiable data to your desktop.

- USB connected hard drives or similar – these drives have the potential to store large quantities of data and therefore will need to be fully encrypted using device encryption and a justified case made for their use. This will only be considered under specific circumstances and users should contact the Information governance team for approval.

- Laptops – are the most common form of mobile device holding mobile data. A laptop that does not have any form of encryption can allow unauthorised access to the data contained on it, and, so, must be protected. It is the user's responsibility to ensure that their laptops have been installed with the encryption software. The IT Department will install and manage the encryption software across all Trust laptops.

- Other mobile devices – including PDA's, IPad, smart phones, USB memory sticks, CD or DVD's. The loss of any of these devices containing sensitive data would compromise the Trust's information security if there was not robust encryption in place. You are responsible to ensure your device is encrypted please contact the IT department in the first instance.

- All Trust owned computing devices shall be fully encrypted.

- Users will only be allowed to write to approved, Trust-owned hardware-encrypted memory sticks. Departmental managers will be responsible for purchasing the Trust's standard USB hardware encrypted memory sticks for staffs that have an identified business need. Departments purchasing such devices will remain responsible for the safekeeping and recovery in the event of staff leaving the organisation as with any other piece of Trust equipment.

21 Text messaging

The Trust recognises that SMS text messaging could co-exist alongside other methods of communicating with patients for several reasons:-

- it is a prompt, reliable, efficient and cost effective method of contacting patients
- the message will go to a contact number provided
- mobile phones are usually personal devices
- there is a traceable proof of sending

Milton Keynes University Hospital NHS Foundation Trust collect mobile phone numbers to contact patients for direct care purposes or dealings with the Trust in order to:-

- arrange appointments

- remind the patient of appointments
- request the patient contact the Trust
- provide information to patients

When communicating verbally with the patient, staff must check:-

- that the mobile number previously given remains current or;
- if no number listed then to request the patient's mobile number, and
- If the patient provides/has provided a mobile number this may be used.

If the patient chooses to provide details of their mobile phone number but not to receive messages, then this information needs to be recorded onto the eCare Administration System.

Patients will be advised to the possible use of the text service at the bottom of appointments letters. Staff must ensure that:-

- Texts will only be sent to patients during the day or early evening, the Trust cannot accept responsibility for delays from messaging providers
- Text messages must not be sent from staff's personal mobile phones
- Messages to patients should have no patient identifiable data enclosed
- Only clear unambiguous messages should be used. All text services will include a method for the patient to contact the Trust e.g. a phone number for contact.
- Texts will be sent to the mobile number supplied.

22 Photography, Video and Audio Recording

The Trust needs to ensure that all recording that takes place within the hospital, whether for the specific purposes of media use or the use of Milton Keynes University Hospital NHS Foundation Trust, or for patient's personal use in limited cases or normal recording for health purposes is done:

- For a clear purpose
- With full consent of all patients and staff
- With appropriate control of use and storage

Recording' includes photographic video recording and audio recording irrespective or media used, images includes both still and moving pictures.

This does not include photography taken by trust systems as part of the patient's healthcare.

- Diagnostic imaging, including PACs
- Images taken from pathology slides
- Laparoscopic treatment where images are real-time and are not retained
- Ultrasound images
  These are covered by specific guidance or the general arrangements for handling medical records
- Audio tapes of dictation/interview notes, which should be wiped clear immediately after transcription and checking

However, it does include:-

- recordings made and used for clinical purposes e.g. as part of the assessment,
- education and training of health professional
- recordings for non-clinical purposes
- Patient initiated recording

While there are many reasons why visual and audio recording can be beneficial, e.g. to assist in treatment; to record changes; for teaching; to inform patients and the public, the hospital's first priority must be to protect the interests and well-being of individual patients and to keep information about patients confidential.

All recording must be managed in accordance with the Data Protection Act 2018, Caldicott Principles, Copyright Laws and Best Practice as detailed in this policy.

Recording Made or Used For Clinical Purposes

Clinical purposes include treatment, assessment, recording disease progression, and teaching.

The Trust's policy is that explicit, informed consent to recording is obtained from all patients in all cases prior to recording taking place.

Where the recording takes place as part of interventional procedure consent may be confirmed by adding a sentence to the standard consent form.

In other cases, for example when recording a consultation, you should seek the patient's explicit consent, using the **Recording Checklist and Consent form** at Consent Form, completed to explain why the recording is being made and how it will be used.

Where recording is required as an integral part of a research project, this must be specifically included in the research protocol. In this situation, the consent to recording may be combined with the consent to take part in the study.

You should be particularly vigilant if you are involved in recording patients who are mentally ill or disabled, seriously ill patients, children, or other vulnerable people, for television or other publicly available media.

Recordings made for clinical purposes form part of the medical record and should be filed within that record at the earliest opportunity. Disclosure of recordings is permissible under the same arrangements as for medical records via the Information Governance Department.

Before the recording, you must ensure that patients:

- Understand the purpose of the recording, who will be allowed to see it, including names if they are known, the circumstances in which it will be shown, whether copies will be made, and the arrangements for storage and how long the recording will be kept

- Understand that withholding consent, or withdrawing consent during the recording, will not affect the quality of care they receive.

- Are given time to read explanatory material and to consider the implications of signing the consent form.

- Understand, where a recording is made for a television programme or other publicly available media that, after the recording process has been completed, those who own the recording are not bound to accept withdrawal of consent to use the recorded material. If they wish to restrict the use of material, they should get agreement to this in writing from the owners of the recording before recording begins.

- Understand that in the case of electronic publication, once the recording is in the public domain, its use cannot be controlled.

When disability or illness prevents patients from giving informed consent, you must get agreement from the next of kin or carer. Where children who lack the understanding to consent are to be recorded, you must get permission from a parent or guardian. People agreeing to recordings on behalf of others must be given the same rights and information as patients acting on their own behalf. Under the data protection act 2018 Children aged 13 and over who have the capacity and understanding to consent to recording may do so. You should make a note of the factors taken into account in assessing the child's capacity.

In exceptional circumstances you may judge that it is in the patient's best interests to film them without first seeking consent. Such circumstances may arise, for example, where you believe a child to be the victim of abuse. Before recording a patient without consent you should discuss your decision with an experienced colleague normally at consultant level and record the decision in the clinical records.

While recordings may be made of patients while unconscious, they can be retained and used only after consent has been obtained subsequently from the patient or their relatives. You must be prepared to justify your decision to the patient and, if necessary, to others.

If you have made a film in the course of treating or assessing a patient, and wish to use it for another purpose e.g. teaching, you must obtain the patient's further consent. You must first ensure the patient understands what the film will be used for, and who will have access to it. In particular, you must not publish or broadcast such film in any form without obtaining explicit, written consent from the patient.

You may use effectively anonymised images for medical education and research and clinical audit without obtaining consent. Blacking out eyes in a facial image is not an acceptable means of achieving this. You must however obtain consent before publishing such film in textbooks or journals or otherwise agreeing to allow public access to them. Where patients can be identified from films which are to be used for clinical audit, education or research within a hospital or other professional medical setting, you should ensure that the patients are informed that the images may be used for these purposes and that they have a right to object.

The procedure to be followed is:

Recording should be approved by the Consultant in charge of the case/head of department.

In all cases, the person responsible for the recording must complete and sign the appropriate checklist/consent form setting out the relevant conditions **Recording Checklist and Consent form** at Consent Form

The patient must be given a copy of the checklist/consent form and the guidance to patients leaflet.

A copy of the consent form should be included in the patient's medical records and a second copy given to the patient. See **Recording on Hospital Premises Flow chart at** Digital Recording Flow Chart

Any image or audio recording should be endorsed with the name of the patient, hospital number and date of capture.

No recording should compromise the patient's privacy and dignity, taking account of religious and cultural factors.

Images should be of the standard necessary to purpose e.g. diagnosis should not be based on the image from a mobile telephone.

Recordings for Non Clinical Purposes

Recording for TV/educational programmes, equipment promotion or similar purposes requires the approval of the Caldicott Guardian / Head of Communications. Recording by other agencies e.g. Police, Health and Safety Inspectors requires approval by the clinician/ departmental Head and the team must inform the Communications Department.

The person responsible for the recording must complete the appropriate checklist setting out the relevant conditions **Recording Checklist and Consent Form – Recording for Non-Clinical Purposes**. Consent Form

Any patients or staff to be filmed must be given a copy of the checklist **Recording Checklist and Consent Form – Recording for Non-Clinical Purposes**. Consent Form, the guidance to patients leaflets Visual, Audio and Digital Recording and sign consent form **Recording Agreement/Indemnity Form at** Consent Form**.** It is recommended that consent is obtained by someone who is not involved in caring for the patient, to ensure that the decision is not influenced by existing relationships.

The consent form must be countersigned by the relevant clinician and a copy should be included in the patient's medical records and one sent to the Communications Department.

If at any time during the recording, staff feel that a patient is uncomfortable or in any kind of distress, they should check that the patient is willing for the filming to continue and if not, stop the filming. Staffs have a veto on medical/welfare grounds on recording.

Where in the view of the staff responsible for their case a patient is unable to consent, the decision to include them in the film will be referred to the Caldecott Guardian who, in consultation with any relative, will come to a view as to whether the benefits outweigh the risks. **Recording on Hospital Premises Flow chart at** Digital Recording Flow Chart

The Information Governance Manager will advise on any variations required to the consent forms.

For safety and security purpose, the Trust has an extensive CCTV system in operation.

Any staff member who consciously breaches these requirements will be subject to appropriate disciplinary investigation.

Patient Initiated Recording or Audio Recording of an Appointment

Where a patient requests that recording of a procedure takes place, e.g. video recording of a birth or audio recording of an appointment, this should be permitted subject to:

- The explicit agreement of the patient and staff members involved
- Confirmation that the recording is for personal use only, see Guidelines for Patients who wish to make a Recording
- No interference with the safe performance of the procedure
- Any third parties potentially included consenting, including staff.
- Agreement that the recording stops immediately at the request of the clinician in charge.

Overt Patient Recordings

Although we cannot place restrictions on a patient wishing to record notes of a consultation or conversation with a health professional, where it is felt absolutely necessary by the patient to do so, we should ensure that :-

- Any recording is done openly and honestly
- The recording process itself does not interfere with the consultation process or the treatment of care being administered
- The patient understands that a note will be made in their health record stating that they have recorded the consultation or care being provided
- The patient is reminded of the private and confidential nature of the recording and that it is their responsibility to keep it safe and secure
- Any recording is only made for personal use
- Patients are aware that the misuse of a recording may result in criminal or civil proceedings
- Patients are discouraged from undertaking recordings in the first place, unless it is deemed absolutely necessary by highlighting the above responsibilities

Covert Patient Recordings

Although we cannot place restrictions on a patient wishing to covertly record a consultation or conversation with a health professional, where organisations are aware that covert recording is a significant issue they should aim to discourage patients from doing so by ensuring that :-

- The organisation promotes the open and honest recording of consultations, where a patient deems it absolutely necessary (see the advice above, which applies equally to covert recording)
- Patients are aware that the organisation takes proactive steps to investigate and address any issues regarding the patient's treatment and care, to avoid them feeling it necessary to record their consultation
- Relevant staff should consider providing patients with a written record summary, and or a verbatim record (if practical) of their consultation for their own personal use
- Patients are advised that they are entitled to see their notes if they so wish, by informally asking the healthcare professional in charge of the consultation, or to request a paper copy of their medical notes formally through a Subject Access Request (SAR) made under the Data Protection Act 2018
- Patients are given information on how they can complain if they have an issue with their treatment and care, and their attention is drawn to the relevant guidance from the Care Quality Commission (see below) and Information Commissioner's Office

Quality Standards - Digital Images

Digital images are easier to copy, manipulate and distribute than traditional recording.
Where digital photography is to be used to record images of patients, due care must be given before the start of the project to ensure that the quality of the image (in terms of both resolution and colour depth) is adequate for its purpose. If an image is manipulated a note must be made of the programme used and manipulation undertaken and enclosed with the image.

In order to maintain the integrity of the image, manipulation must be limited to simple sharpening, adjustment of contrast and brightness and correction of colour balance.
Images of patients must not be transferred to personal computers, except for the preparation of teaching materials; these must not contain personal identifiable information. Images must be removed once the materials have been completed and must not be forwarded to third parties.

Staff acquiring copies of recordings in the course of their duties may retain these for teaching purposes, but must undertake only to use them within the terms of the original consent. Copyright and reproduction rights at all times remain with Milton Keynes University Hospital NHS Foundation Trust.

Recording for Media/Communication Purposes

This will take place only with the agreement of and under the control of the Head of Communications, who will be responsible for obtaining all appropriate consents and assurances including consent from patients. Staff approached direct should refer the request to the Head of Communications, and staff should challenge anyone on the site who appears to be filming for such purposes to ensure that appropriate consent has been obtained.

Processing, Retention and Storage

Film processing must only be carried out by a laboratory who has signed our Third Party Agreement.
Patient related recordings, under the requirements of the Data Protection Act, must be kept only for as long as they are needed, and must be available for disclosure to the patient when needed.

Recordings made for assessment/treatment will be held in the patient's medical records.

Other patient recordings must be kept systematically and securely, together with the relevant paperwork, and destroyed at the end of the agreed period as confidential waste.

Where digital images are stored on a PC, access must be restricted to those who have a clinical need to see the images and password protected.

23 Smartcard Security

Authorised users of smartcards are required to observe the following security practices:

- Keep smartcards secure. Do not store card and PIN number together.
- Do not share Smartcards or pass codes with other users.
- Report any observed instances of others abusing the Smartcard system.

Lost, Stolen and Broken Smartcards

Lost and damaged Smartcards should be reported to the IT service desk immediately and a new card requested by completing the relevant documentation.

Smartcard Misuse

All users digitally sign a Smartcard Terms and Conditions agreement when issued with their Smartcards. If a user fails to comply with these Terms and Conditions then appropriate disciplinary measures will be taken.

24 Mobile Computing

In recent years there have been significant advances in mobile technologies. To coincide with this mobile devices have gained wider acceptance in the consumer market and in the workplace. Today portable devices such as smart phones, tablet devices, notebooks, laptops etc. are in wide circulation.

The Trust will allow mobile devices, which includes both Trust owned and staff owned mobile equipment, to access its information assets. For minimum levels of security that need to be applied please see IT Policy

Access from Public Areas

Staff should show due diligence when accessing any Trust data in public areas using either Trust owned or public devices e.g. Internet Cafés and must ensure that any information accessed remains safe and secure. Also any equipment being used must not be left unattended at any time.

Access from Business Areas (e.g. NHS premises)

Staffs are responsible for ensuring that no unauthorised individuals are able to see information or access Trust systems. If equipment is being used outside of its normal location and might be left unattended, the user will secure it by other means (such as security cable, locked cabinet or room).

Remote Access

The Trust provides remote access to both staff and third parties via a Virtual Private Network (VPN) or the TAC Portal. Please refer to relevant IT Policy
Use of any information at home must be for work related purposes only.

- Staff must ensure the security of information within their home. Where possible mobile devices and storage media should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored in a way that it is not obvious to other members of the household.

- Staff must ensure the security of any mobile data device, business critical information and personal identifiable data in transit to their home.

Mobile Device Cameras

The use of Trust owned or personal mobile devices for taking photographs for business related purposes is permitted but must take into account the following guidance and staff must ensure that they have the agreement of the Caldicott Guardian in relation to the use of any images taken.

In relation to this any individual taking a photograph of another individual using their mobile device, will be processing personal data and must comply with the Data Protection Act 2018

Where a photograph contains personal data it will be necessary for the individual being photographed to give their explicit consent to the photograph being taken and should also be notified of all the purposes for which the photograph will be used.

All images must be deleted from the mobile device and placed in the medical records if applicable.

Transport of Equipment, Files and Paper Documents

Staffs are responsible for ensuring safe transport when removing equipment, files and data from Trust premises.

- IT equipment must be transported in a secure, clean environment. Equipment is not insured and you may be held liable if you do not take reasonable precautions.
- Equipment, and paper files should be kept out of sight (in car boots), locked away and not be left unattended at any time.
- Appropriate packaging such as sealed envelopes, bubble wrap etc. will be used to prevent physical damage.

Where a courier service is used to transport packages containing sensitive information tamper proof packaging will be used. Courier firms should guarantee the safe arrival of parcels and the confidentiality of any contained information. Please see our approved courier list on Trust intranet.

25 Copyright

The main legislation dealing with copyright in the United Kingdom is the Copyright, Designs and Patents Act, 1988. This section ensures that all staff, volunteers and contractors are aware of their individual responsibilities in relation to this.

It is the responsibility of each and every employee of Milton Keynes University Hospital NHS Foundation Trust, volunteers and contractors, to comply with this licence. Anyone found to be infringing copyright intentionally may be subject to disciplinary action.

Photocopying
The Licence permits photocopying from a very wide range of publications. You can copy from works published in the UK and Mandating Territories and by Participating US Publishers. You cannot copy from Excluded Works, and works in any Excluded Category.

Scanning
The Licence permits scanning from a very wide range of publications. You can make Digital Copies from print Works published in the UK and other countries with which CLA has agreed a 'Digital Repertoire Exchange' as listed on www.cla.co.uk and updated from time to time. You can make Digital Copies of any U.S. Work listed as being available for copying on the CLA website www.cla.co.uk, as long as an electronic copy is not readily available from the publisher. On each occasion you may only copy up to two articles from a periodical. You cannot copy from Excluded

Works, and works in any Excluded Category.

Digital Copying
You can make Digital Copies from UK publications created and distributed in electronic form published by a Participating Digital Material Publisher except Excluded Works or works in any Excluded Category. You can make Digital Copies of any U.S. work created and distributed in electronic form listed as being available for copying on the CLA website http://www.cla.co.uk. On each occasion you may only copy up to two articles from a periodical. You cannot copy from Excluded Works, and works in any Excluded Category.

The main categories of works currently protected in the UK include:

- original literary works such as novels or poems, tables or lists and computer programs
- original dramatic works such as dance or mime
- original musical works, i.e. the musical notes themselves
- original artistic works such as graphic works (paintings, drawings etc.), photographs and sculptures
- newspapers
- sound recordings
- films
- broadcasts / podcasts
- typographical arrangements (i.e. the layout or actual appearance) of published editions

What can I use copies for?

- To share with colleagues at meetings or briefings
- For internal training purposes, e.g. journal clubs, nurse teaching sessions, students on placement etc.
- To share media coverage within your organisation
- For Health & Safety or Environmental Awareness
- For research and development

A patient or carer may receive a single paper copy of content relevant to their treatment.

Printed books and journals

You may make paper copies and scanned copies from **most** printed journals and books under the terms of the NHS CLA Licence *****

- Copies must be for NHS staff and for NHS purposes
- You may copy two articles from a journal issue (more if it is a thematic issue), one chapter from a book or 5% of above, whichever is greater
- Within these extent limits, you can make multiple copies
- Single paper copies relating to a patient's condition or treatment may be made for patients and carers
- Scanned copies may be sent via NHS e-mail but not placed on web sites; scanned copies can be used in Power Point presentations
- You should always acknowledge the source of your copies
- No copies may be made from newspapers

Electronic works

You normally may only download and print material for the purposes of:

- private study
- non-commercial research
- non-commercial purposes
- Always check copyright notices on websites
- E-journals are covered by publisher licences

You may not copy images, sounds or any other electronic media without permission

IT Security and Software Licensing

The Act provides the same rights to authors of computer programmes as literary, dramatic and musical authors have to their works. Those rights extend for the life of the author and for seventy years after the author's death.

Software is generally not sold outright to the user. Instead the user is granted the right to use it as laid down in the user licence. It is normally expected that only one person at a time will have access to and use the software concerned. A network licence may be purchased, normally at a reduced rate, for a defined number of users. A site licence may be available to cover all (unlimited) users within the premises.

It is thus illegal to make copies of software without the copyright owner's consent, or to duplicate software loaded on a hard disk for use on any other personal computer unless allowed for under the licence.

Likewise it is not permitted to copy or download or upload music files (including MP3s), or to download other electronic media such as DVD files etc. which may be subject to copyright legislation, onto Trust equipment without explicit permission from the information Governance Manager or the Head of IT.

Copyright Ownership and the Trust

Management consultants, agency staff and other independent contractors, who are being commissioned/paid by the Trust but who are not members of staff, automatically hold the copyright of works they produce during this time. Because of this it is imperative that all managers who engage consultants ensure that they have signed a contract which states that they agree to the Trust holding the copyright of any documentation or other products produced by them on completion of their contract with the Trust.

Copyright on any documentation, presentations etc. produced by staff employed by MKUHFT as part of their contractual work remains the copyright of the Trust unless there is a specific contract in place for the copyright to remain with the Author.

Breach of Copyright

It is an infringement of copyright to do any of the following acts in relation to a substantial part of a work protected by copyright without the consent or authorisation of the copyright owner:

- copy it
- issue copies of it to the public
- rent or lend it to the public
- perform or show it in public

26 Freedom of Information

The Freedom of Information Act 2000 ("The Act") is part of the Government's commitment to greater openness in the public sector.

The main features of the Act:

- A general statutory right of access to all recorded information held by public authorities, subject to certain conditions and exemptions.
- Anyone who writes or emails the Trust and asks for information will have the right to be told whether or not the Trust has the information, and if so, have that information communicated to them.
- There are exemptions in the Act which specify the circumstances in which the Trust may consider whether information should be withheld.
- The Trust has a duty to publish and maintain a Publication Scheme which provides as much information about the activities of the Trust as is reasonably practicable so that members of the public do not have to make a formal request.
- Under the Environmental Information Regulations there are separate rights of access to information about the environment.

General Rights of Access to Recorded Information

The Trust has produced a Guidance leaflet to help any applicant who may wish to make a request for information; these are available within all Departments and can be found on the Trusts intranet and internet.

The Trust accepts that all written requests for information are potentially FOIA requests save where the information is available through the Publication Scheme. However the provision of advice and assistance to members of the public about every aspect of the health services which the Trust provides is part of the day to day business process of the Trust. A key element of the Trust's policy is that the release of information does not become cumbersome, time consuming or resource intensive. The Trust therefore expects that written requests for information, which are part of the day to day business of the Trust, will continue to be handled in the normal way.

In accordance with the Act, the request must be in writing, stating the name of the applicant and an address for correspondence, which sets out the information requested. For the purpose of general rights of access, a request is to be treated as made in writing if it is transmitted by email and includes an email address for subsequent reference.

Time Limits for Compliance with Requests

The Trust has established appropriate systems and procedures to ensure that the organisation complies with the duty to confirm or deny and to provide the information requested within 20 working days.

All FOI requests must be passed through the Executive Directors before going out and MUST be sent to the requester within 20 working days. If you receive a request from the Information Governance/Freedom of Information Co-ordinator for information please ensure that you respond within 10 working days.

Unreasonable delays in responding to this request will be reported to the relevant Director for. Delays and poor FOI performance ultimately reflects on the Board and its Directors and could

result in the Trust receiving an Enforcement Notice from the office of the Information Commissioner.

27 Disposal

Data Devices

This Section details the Milton Keynes University Hospital NHS Foundation Trusts procedure for secure disposal or re-use of Data Devices that are to be re-deployed within the Trust or disposed of as Beyond Economical Repair (BER) or excess to requirements and are subsequently to be scrapped.

The Trust has a legal duty to ensure that all information is securely handled and only accessed on a need to know basis. In order to conduct this duty of care from 'cradle to grave' the Trust is required to ensure that when equipment is re-deployed or disposed of all information is either removed or destroyed, this includes computer files, the computers themselves, disks and USB sticks, in line with the Computer Misuse and Data Protection Acts.

It is the responsibility of the user to ensure that all CD/DVDs or USB memory sticks are taken, in person, to the IT department for secure disposal.

For further information and disposal please contact the IT Department on 01908 997000 (ext. 87000).

Medical Devices

Some medical devices stores personal identifiable data within the equipment. These devices must be wiped of all data before they are sent for disposal/re-use. Please refer to Condeming,Transfer & Disposal of Medical Devices for further guidance

Information held in paper form

It is important that personal identifiable/business critical information is disposed of in a secure manner.

Blue Shredding bins have been provided for all confidential waste and these bins are emptied and shredded on site on a fortnightly basis to ensure security and confidentiality is maintained, for adhoc requests please contact the Information Governance Team on 01908 995044 ext. 85044.

Staffs are reminded that information must not be removed from site unless there is a justified clinical reason which has been approved as part of the patient flows. It is essential staff ensure items such as handover sheets, patient identifiable sticky labels, ward lists and messages are shredded at the end of each shift and not removed from site.

28 Retention of Records

Milton Keynes University Hospital NHS Foundation Trust recognises the need for robust governance around the retention and storage of records and therefore adopts the Department of Health's "Records Management Code of Practice" to ensure that our information remains available, confidential and up to date at all times.

This policy covers both clinical and non clinical records.

Details of this policy can be found at Retention of Records Guide

29 Audits

All clinical audits must adhere to NHS information governance policies and standards. Audits should pay special attention to the Data Protection Act 2018/GDPR and the Caldicott Principles (1997). This means, for example, that data should be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal

The Trust expects all staff involved in clinical audit to follow the above principles and to ensure that patient-related data is collected, stored and reported on in a non-identifiable manner. No data should be collected until the audit proposal is approved.

Data collected for audit purposes should be disposed of in a secure manner in line with the Trust Health Records policy when the relevant group has ratified the report emanating from the data as final.

Data collected for audit purposes is considered to be Trust (not personal) property. Thus, where an individual undertaking an audit leaves post prior to completion of data collection/report writing, the data should be transferred to the Compliance & Audit Manager /Clinical Governance Department or keep them informed of any alternative arrangements that have been made.

When presenting data within a report, it is generally appropriate to display by, for example, ward or team. However, the Trust considers it inappropriate to name – or otherwise seek to identify – individual staff within an audit report (the purpose of clinical audit being quality assurance and improvement, not performance management).

When finally approved, clinical audit reports are placed on the Clinical Governance Department pages of the MKHFT Staff Intranet. These pages are maintained by the Clinical Governance Department and uploaded on a Read Only basis. Reports remain available on these pages for a five year period in line with Department of Health Records Management: NHS Code of Practice parts 1 (2006) & 2 (2009).

30 Breaches of this Policy

Any breach of this policy may result in the Trust's disciplinary policy being invoked. This may lead to suspension and dismissal.

31 Relevant acts of Law & Best Practice

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

The Privacy and Electronic Communications Regulations (PECR)

They are derived from European law and implement the European Directive also known as 'the e-privacy Directive'.

The e-privacy Directive complements the existing data protection regime and sets out more-Specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy.

PECR sits alongside the Data Protection Act 2018. They give people specific privacy rights in relation to electronic communications.

PECR will apply if you:

- Market by phone, email, text or fax;
- Use cookies or a similar technology on your website; or
- Compile a telephone directory (or a similar public directory).

Human Rights Act 2000

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take individuals rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act came into force in November 2000 and will be fully in force by November 30th 2005. The Information Commissioner (previously the Data Protection Commissioner) will oversee the implementation of this Act. This Act gives individuals rights of access to information held by public authorities. Further information will be available as implementation progresses.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each user an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records 1990

This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Health and Social Care Act (2000)

Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer programs) Regulations 1992)

The NHS Care Record Guarantee
The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to patients' rights to access their information, how information will be shared both within and outside of the NHS, and how decisions on sharing information will be made.

NHS Code of Practice
The NHS Code of Practice provides the basis for reliable and effective information security management by NHS organisations, and is equally applicable to those organisations that may share in NHS information resources of all kinds. This Code of Practice is an integral component within the overall NHS Information Governance Programme.

NHS GUIDANCE

The NHS IM&T Security Manual Ensuring Security & Confidentiality in NHS Organisations

Provides detailed instructions for NHS bodies to comply with security requirements to protect an individual's confidentiality and the security of Trust information systems.

The Protection & Use of Patient Information

Gives NHS bodies guidance concerning the use and protection necessary for patient information. It also considers ways of obtaining and using patient information to comply with Data Protection legislation, current and planned.

Caldicott Guardians & Implementing the Caldicott Standard into Social Care

Provides guidelines relating to sharing of patient identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance.

For the Record

Provides guidance to improve the management of NHS records explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as patients, employees, volunteers etc.

Information Security Standards

This is the accepted industry standard for Information Management and Security. This standard has been adopted by the NHSE and all NHS organisations now have to ensure compliance with

these requirements. It is also a legal requirement under the notification and principle 7 of the Data Protection Act.

32 Contact IG Team

Information Governance Manager/DPO	85041/ Bleep 1503
Deputy Information Governance/Security Manager	85045/ Bleep 1731
Information Governance Officer	85044 /Bleep1731
Information Governance Officer (Freedom of Information)	85043/ Bleep1731
Information Governance Administrator (Access to Health Records)	85042 /Bleep 1731

Document review history

Version number	Review date	Reviewed by	Changes made
01	**January 2014**	**Dawn Budd**	**New Policy – combining all IG policies**
02	**January 2015**	**Dawn Budd**	**Amendment to include the PIA & SAA**
03	**Sept 2015**	**Dawn Budd**	**Minor amendments i.e. logo, telephone numbers**
04	**October 2016**	**Dawn Budd**	**Addition of What's App**
4.1	**January 2016**	**Dawn Budd**	**Minor amendments – typo's**
4.2	**December 2017**	**Dawn Budd**	**Minor amendment - encryption**
5.	**March 2018**	**Dawn Budd Heidi Walker**	**Full overview of policy for the DPA 2018 inc GDPR**
5.1	**January 2019**	**Dawn Budd**	**Minor changes to incorporate the new toolkit and remove the old one.**

Consultation History

Stakeholders Name/Board	Area of Expertise	Date Sent	Date Received	Comments	Endorsed Yes/No
Information Governance Team		3-2-14	11-2-14 14-2-14	Minor Amendments	

Information Governance Steering Group		11-2-14	20-2-14	Minor Amendments	
IT		3-2-14	4-2-14	Minor Amendments	
Data Quality		3-2-14			
IGSG	Information Governance	22-1-15	23-1-15	Amendments to include PIA & SAA	
IGSG	Information Governance				
Dawn Budd	Information Governance	Jan 2016	Jan 2016	Minor Amendments	
Dawn Budd	Information Governance	Dec 2017	Dec 2017	Minor Amendments	
IGSG	Data Protection/Information Governance	March 2018		Full overview of policy for the DPA 2018 inc GDPR	

Audit and monitoring

Document Audit and Monitoring Table	
Monitoring requirements:	a) Compliance with information governance agenda across the organisation. Ensure training is undertaken by all staff
Monitoring Method:	a) Reports and audits and IG Toolkit
Monitoring prepared by:	a) Information Governance Steering Group
Monitoring presented to:	a) Management Board b) Trust Board c) Audit Committee
Frequency of presentation:	a) Annually

Equality Impact Assessment

As part of its development, this policy and its impact on equality has been reviewed. The purpose of the assessment is to minimise and if possible remove any disproportionate impact on the grounds of race, gender, disability, age, sexual orientation, religion or belief, pregnancy and maternity, gender reassignment or marriage and civil partnership. No detriment was identified.

Equality Impact Assessment			
Division	**Corporate**	**Department**	**Information Governance**
Person completing the EqIA		**Contact No.**	
Others involved:		**Date of assessment:**	**15/05/2018**
Existing policy/service	Information Governance Policy	**New policy/service**	**Information Governance Policy**

Will patients, carers, the public or staff be affected by the policy/service?	Staff
If staff, how many/which groups will be effected?	All staff

Protected characteristic	Any impact?	Comments
Age	NO	
Disability	NO	
Gender reassignment	NO	
Marriage and civil partnership	NO	
Pregnancy and maternity	NO	
Race	NO	
Religion or belief	NO	
Sex	NO	
Sexual orientation	NO	

What consultation method(s)	

have you carried out?	
How are the changes/amendments to the policies/services communicated?	