DATA PROTECTION, CONFIDENTIALITY AND SECURITY POLICY

Version	Date	Purpose of Issue/Description of Change	Review Date
1	Sept	Amalgamation of the Policy in Respect of Confidentiality of Patient Information and Safe Haven's & Communication of Personal Information Policy	June 2021
1.1	Dec 2014	Minor amendment	
2	Sept 2015	Review and update	
3	July 2017	Review and update	
4	May 2018	Complete rewrite and rename. Amalgamation of Confidentiality and Security of Personal Information Policy and Information Risk Management Policy	

Status	Open	
Publication Scheme	Our Policies and Procedures	
FOI Classification	Release without reference to author	
Function/Activity	Information Governance	
Record Type	Policy	
Project Name	N/A	
Key Words	Information Governance, Confidentiality, Patient Information, Personal Information, Staff Information, Sensitive Information, Data Protection, Information Security	
Standard	Data Security and Protection Toolkit	
Author	Information Governance Manager	**Date/s**
Approval and/or ratification body	Data and Information Governance Steering Group	26th June 2018

CONTENTS

1. INTRODUCTION

Everyone working for or on behalf of the NHS has a duty to keep information about patients, carers, clients, staff and other individuals confidential, and to protect the privacy of information about individuals.

1.1 Purpose

The purpose of this policy is:

- To ensure any personal information collected and held by the Trust is processed fairly and lawfully.
- To promote best practice in the processing of personal information.
- To ensure that Trust staff involved in processing personal information understand their responsibilities and obligations.
- To ensure that Trust staff responsible for the processing of personal information are adequately trained to fulfil their responsibilities and obligations.
- To outline the procedure for reporting and investigation of a suspected breach of Confidentiality and/or Data Protection.
- To provide assurance to our patients, staff and others with whom we deal that their personal information is processed lawfully and correctly and held securely at all times.

1.2 Scope

This policy relates to all types of information within the Trust. These include:

- Patient/Client/Service User information
- Personnel information
- Organisational information.

1.3 Definitions

Personal Information

Personal Information is information which can alone or in combination with other information identifies an individual. Examples are:

- surname, forename, initials, address, postcode
- NHS number, unit number, National Insurance number

Sensitive Personal Information

Sensitive personal information is data that contains details of a person's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life

- sexual orientation

Data Subject
A data subject is the person who is the subject of the information.

Data Controller
A data controller is the individual, company or organisation that determines the purpose and the manner in which personal information may be processed.

Data Processor
A data processor processes the personal information on behalf of a data controller.

Data protection legislation
Within this policy, 'data protection legislation' shall be taken to mean all relevant legislation; some are detailed in section 2.

Information Assets
Information Assets are pieces of information that are valuable to the organisation, such as databases, data files, contracts and agreements, and archived information.

Information Asset Owner
Information Asset Owners are nominated to help achieve and monitor a robust Information Governance culture across the Trust, address risks to the information assets they 'own' and to provide assurance to the Senior Information Risk Owner on the security and use of these assets.

2 LEGAL FRAMEWORK

2.1 Caldicott Principles

The Caldicott Principles represent best practice for using and sharing identifiable personal information and should be applied whenever a disclosure of personal information is being considered.

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

2.2 Data Protection Act

The Data Protection Act sets out six principles:

a) processing be lawful and fair
b) purposes of processing be specified, explicit and legitimate
c) personal data be adequate, relevant and not excessive

d) personal data be accurate and kept up to date
e) personal data be kept for no longer than is necessary
f) personal data be processed in a secure manner

2.3 General Data Protection Regulations (GDPR)

General Data Protection Regulations 2016 is a legal set of rules that be adhered to by organisations that process, harvest, store or make use of personal information. The focus is on people. It grants people rights and places the obligation on organisations that hold their data. The GDPR sets out seven key principles:

a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimisation
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality (security)
g) Accountability

2.4 Common Law Obligations

The Common Law Duty of Confidentiality position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

2.5 NHS Care Record Guarantee for England

The Care Records Guarantee sets out high-level commitments for protecting and safeguarding patient information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

2.6 NHS Code of Practice on Confidentiality

The NHS Code of Practice on Confidentiality is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

2.7 NHS Code of Practice on Information Security Management

The NHS Code of Practice on Information Security Management is a guide to the methods and required standards of practice in the management of information security for those who work within, under contract to, or in business partnership with NHS organisations in England. Its purpose is to identify and address security management in the processing and use of NHS information and is based on current legal requirements, relevant standards and professional best practice.

2.8 A Guide to Confidentiality in Health and Social Care

The Health and Social Care Information Centre has produced a Guide to Confidentiality in Health and Social Care which explains the various rules about the use and sharing of confidential information. It has been designed to be easily accessible and to aid good decision making. It also explains the responsibility organisations have to keep confidential information secure.

2.9 The NHS Act

Section 251 of the NHS Act enables the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant without the discloser being in breach of the common law duty of confidentiality. The Confidentiality Advisory Group (CAG) review applications and advise whether there is sufficient justification to access the requested confidential patient information. Using CAG advice as a basis for their consideration, the Health Research Authority or Secretary of State will take the final approval decision.

2.10 Health and Social Care (Safety and Quality) Act

The Health and Social Care (Safety and Quality) Act supports the sharing of information relating to an individual for the purposes of providing that individual with health or social care services in England;

2.11 NHS Constitution for England

The NHS Constitution for England states that patients *"have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure"*

2.12 NICE Clinical Guideline 138 and Quality Standard 15

Under the NHS Standard Contract a provider must at least once in each contract year audit its practices against quality statements regarding data sharing set out in NICE Clinical Guideline 138. Quality Standard 15 contains the quality statements:

- Quality Statement 12: Coordinated care through the exchange of patient information
- Quality Statement 13: Sharing information with partners, family members and carers

2.13 Care Professionals' Code of Practice

Care professionals must also comply with the codes of practice of their respective professionals.

2.14 Human Rights Act

Article 8.1 of the European Convention on Human Rights enshrined in Schedule 1 of the Human Rights Act, provides that "*everyone has the right to respect for his private and family life, his home and his correspondence.*" This is however, qualified by

reasons where it may be legitimate to infringe this right. As stated in Article 8.2, these are "*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 of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

The right to privacy will be respected unless it can be shown that there is a legitimate reason to infringe those rights.

2.15 Statistics and Registration Service Act

The Statistics and Registration Service Act permits NHS organisations to submit 'patient registration information' to the Statistics Board for the production of population statistics. This means information about individuals who are or have been registered in England or Wales to receive primary medical services. The information includes:

- address and any previous address
- date of birth and sex
- patient identification number
- history of registration

Information about the health or condition of, or the care or treatment provided, is specifically excluded from disclosure and must not be shared with the Statistics Board.

3 DATA PROTECTION AND CONFIDENTIALITY

Data protection legislation covers living individuals but we must still uphold the confidentiality of the deceased.

All processing of information must be carried out in line with data protection legislation along with relevant guidance identified in section 2.

3.1 Lawful Processing Conditions

A lawful basis is required to process personal information. GDPR sets out the lawful processing conditions. When processing special category data we need to satisfy a special category condition.

3.2 Individual Rights

Individuals have rights under the GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object

8. Rights in relation to automated decision making and profiling.

However there are exceptions to the rules that allow data controllers to refuse a request from a data subject.

4 SECURITY

Appropriate organisation, physical and technical measures need to be adhered to in order to keep information secure.

4.1 Organisational

4.1.1 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is mandatory in most cases when designing or modifying a process that involves personal identifiable information. The objective of a DPIA is to identify risk to personal identifiable information and to then minimise or prevent unlawful processing and data breaches.

The Data Protection Impact Assessment Template contains screening questions for if you need to complete the rest of the DPIA.

4.1.2 Information Asset Risk Assessment

There is a requirement to hold an information asset register that includes all information assets. Each information asset is allocated an Information Asset Owner and Information Asset Administrator who review the asset's Risk Register and Information Asset Risk Assessment, on an annual basis. An annual report is then provided to the Senior Information Risk Owner at the Data and Information Governance Steering Group (DISSG).

4.1.3 Information Flows (data mapping)

As part of the Data Security and Protection Toolkit there is a requirement to identify and risk assess all flows of personal information. This is done on an annual basis and is coordinated by the Information Services Team. An annual report is then provided to the SIRO at the DISSG.

4.1.4 Business Continuity Plans

Where required, systems and processes must have Business Continuity Plans in place. These plans must include testing.

4.1.5 Information Sharing Protocol and Agreement

It is necessary for a sharing agreement and protocol to be completed and signed by the Caldicott Guardian/Data Protection Officer and Senior Information Risk Owner when routinely sharing information with other organisations especially for non-care purposes.

The Trust requires an Information Sharing Protocol with each organisation and an Information Sharing Agreement for each separate request for sharing of information.

- Information Sharing Protocol Template
- Information Sharing Agreement Template

4.2 Physical and Technical Measures

4.2.1 ID badges

- ID badges must be worn and kept secure.
- Report any lost or misplaced ID badges immediately to the General Office.

4.2.2 Restricted areas

- Ensure you check that people are allowed into the area.
- Ensure that no one following you into the area.

4.2.3 Swipe access

- Ensure swipe access is in working order and report to Estates immediately if it is not.
- Ensure staff have the correct access levels, update as appropriate when staff change roles.
- Ensure that the appropriate forms are completed to terminate swipe access when staff leave the organisation.

4.2.4 Door codes

- Door codes should be changed periodically.

4.2.5 Office

- If required ensure your office is locked when unoccupied.
- If required operate a clear desk policy.
- If required lock filing cabinets when not in use.

4.2.6 CCTV

The Trust uses CCTV in some of its premises.

4.2.7 Disposal

- Dispose of confidential waste appropriately.
- Confidential waste must not be used as scrap paper.

4.2.8 Transport

- When transporting personal or confidential information ensure that it is safe and secure at all times.

- Ensure that it is transported in a suitable container.
- Personal or confidential information must remain in your sight or locked securely your car and must be out of sight.

4.2.9 Home/Personal Devices

- You must not take personal or confidential information home without the express consent of your manager.
- Personal or confidential information must remain in your sight or locked securely away.
- Information must not be transferred or stored on personal devices.
- Personal devices must not be used to connect to the Trust's network via VPN

4.2.10 Post

- You must double check the full postal address of the recipient and ensure that you are using the most current contact details.
- Ensure envelopes which contain personal or confidential information are marked "Private and Confidential".
- Chose the most appropriate secure method when sending personal or confidential information.
- Ensure envelopes and packages are sealed efficiently.
- When sending CDs and other removable media they must be encrypted if they contain personal identifiable information.
- Open post away from a public area.

4.2.11 Telephones

- Be careful when leaving messages on answer phones.
- The identity of the caller should always be verified by checking the phone number, and any other relevant details, for example if a patient is calling check date of birth etc., and call back so that the identity can be fully verified. In the case of an organisation, the switchboard number should be used to call back, not a direct dial number.
- If answering machines are used by departments they should be setup so that messages left are recorded silently. This will ensure that no unauthorised personnel overhear confidential messages whilst they are being recorded.

4.2.12 Fax machines

- The fax machine should be sited in a secure location where access to the machine is controlled.
- You should always use a fax cover sheet.
- Check the fax number is correct before sending.
- Only send personal or confidential information when absolutely necessary.

4.2.13 System Access

- Ensure staff have the correct access levels, update as appropriate when staff change roles.
- Ensure access is removed when staff leave the organisation.
- Do not use anyone else's login.
- Ensure you log out of systems when you are not using them.

4.2.14 Passwords

- Do not share passwords.
- Keep your password confidential.
- Change your password periodically.

4.2.15 Smart Cards

- Ensure that the appropriate forms are completed to terminate swipe access when staff leave the organisation.
- Do not leave unattended.

4.2.16 PCs, Laptops, Handheld Devices

- Log off or use password protected screensaver when unattended.
- Ensure it is located where people can't see the screen if in public area.
- Inform IT immediately if missing, lost or stolen.

4.2.17 Removable Media such as memory sticks, CDs

- Any removable media must be virus checked by IT before use.
- Only Trust memory sticks can be used to store personal or confidential information.
- Do not attach any devices unless approved by IT. This includes charging phones and other devices through PC or laptop.

4.2.18 Emails

- All emails are scanned for virus's, on entering or leaving the Trust email server.
- Personal or confidential information should only be sent via email securely. See section 4.3 for further guidance.
- Be aware of phishing emails.
- Be careful of clicking on links as they may not be what they say.
- If you believe you have received a phishing email contact the IT Helpdesk immediately. Do not forward the email.

4.2.19 Printers

- Only print what is necessary.
- Ensure that you select the correct printer.

- Do not leave the printer until you are sure that all the information has printed.

4.2.20 Photocopying

- Do not make excessive copies.
- Do not leave the photocopier until you are sure that all the information has printed.
- Do not leave original or photocopied information on the photocopier.

4.2.21 Scanning

- Do not leave personal or confidential information on the scanner.

4.2.22 Anonymisation & Pseudonymisation

Please refer to the Pseudonymisation & Anonymisation of Data Policy for further guidance.

4.3 Safe Transfer of Personal or Confidential Information

When transferring any personal or confidential information you must:

- ensure the person is entitled to receive the information
- use the most appropriate method to ensure that the information is transferred securely
- limit the information to only what is required, irrelevant information must be removed or redacted (blocked out) before the transferring
- ensure that you are sending information to the correct location
- ensure that no additional information is sent in error
- only send information to those who are entitled to receive it
- mark it 'Private and Confidential'

4.3.1 Post

- Incoming mail must be opened away from public areas.
- All mail must be checked before posting to ensure it is going to the correct address and that nothing additional has been put in the envelope in error.
- All mail that contains personal or confidential information must be enclosed in a sealed envelope and marked 'Private and Confidential', addressed correctly.
- All mail containing sensitive personal or confidential information must be sent via Special Delivery or by a courier (TNT)
- Bulk amounts of personal or confidential information must be sent via Special Delivery or by a courier (TNT)

4.3.2 Email

- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password

- You should not set up your emails to be automatically forwarded to another account, you should set up an out of office to identify who emails should be forwarded to

For HDFT to HDFT or NHS.net to NHS.net

- You must check you are sending the email to the correct email address
- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password
- You must not send the password in the body of the email or a following email. You must contact the person you are sending the email to and confirm the password.

For HDFT to any email address

- You must check you are sending the email to the correct email address
- Any confidential or sensitive information **cannot** be sent from a HDFT account. You must use a NHS.net account so that the email can be encrypted.

For NHS.net to any email address

- You must check you are sending the email to the correct email address
- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password
- You must not send the password in the body of the email or a following email. You must contact the person you are sending the email to and confirm the password.
- Send the recipient the and Receiver Guidance before emailing them the confidential or sensitive email
- Then follow these instructions to encrypt the whole email Sender Guidance

4.3.3 Verbal

- The identity of the enquirer must always be verified by checking the any relevant details. For example if it is a patient ask them to confirm their date of birth, address, and attendance dates etc. If the enquiry is via the phone, call them back so that the identity can be fully verified. In the case of an organisation, the switchboard number must be used to call back, not a direct dial number.
- If answering machines are used by departments they should be setup so that messages left are recorded silently. This will ensure that no unauthorised personnel overhear confidential messages whilst they are being recorded.

4.3.4 Fax

Sending

- By each fax machine there should be a laminated copy of the Fax Flow Chart (Guidelines for Sending Secure Faxes) which acts a prompt to follow the correct procedures when sending a fax.
- All external faxes must use the Trust's Fax Cover Template

- All faxes, internal or external, containing patient information or other confidential information must use the Trust's Fax Cover Template
- Check the recipients fax number, memory alone must not be relied on when dialling. It is acceptable to pre-programme commonly used fax numbers into the machine's memory. However, a list of speed dial numbers must be prominently displayed next to the machine.
- Check if the fax machine is a Safe Haven. If it isn't telephone the recipient of the fax let them know that you are about to send a fax containing confidential information and ask if they will wait by the fax machine whilst you send the document and acknowledge the receipt of the fax.
- Dial the number carefully.
- Monitor the transmission.
- Stop the transmission if there appear to be any anomalies with the transmission.
- Obtain a printed record of the transmission where possible.
- No paperwork must be left unattended at the fax machine.
- If a published fax number turns out to be incorrect, inform all interested parties of the error and amend the list as necessary.

Receiving

- The recipient should remove the fax from the machine on receipt.
- Where necessary, the recipient should contact the sender to confirm receipt and that the fax will be appropriately dealt with and safely stored.

5 REPORTING DATA BREACHES

Data breaches typically fall into the following categories:

- Accidental or unlawful destruction, loss or alteration
- Unauthorised disclosure
- Unauthorised access

All breaches are reported using Datix in accordance with the Identification, Reporting and Management of Incidents Including SUIs.

GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner Office within 72 hours of becoming aware of the breach if there is a risk to people's rights and freedoms. Therefore it is important that all data breaches are reported via Datix as soon as they have been identified.

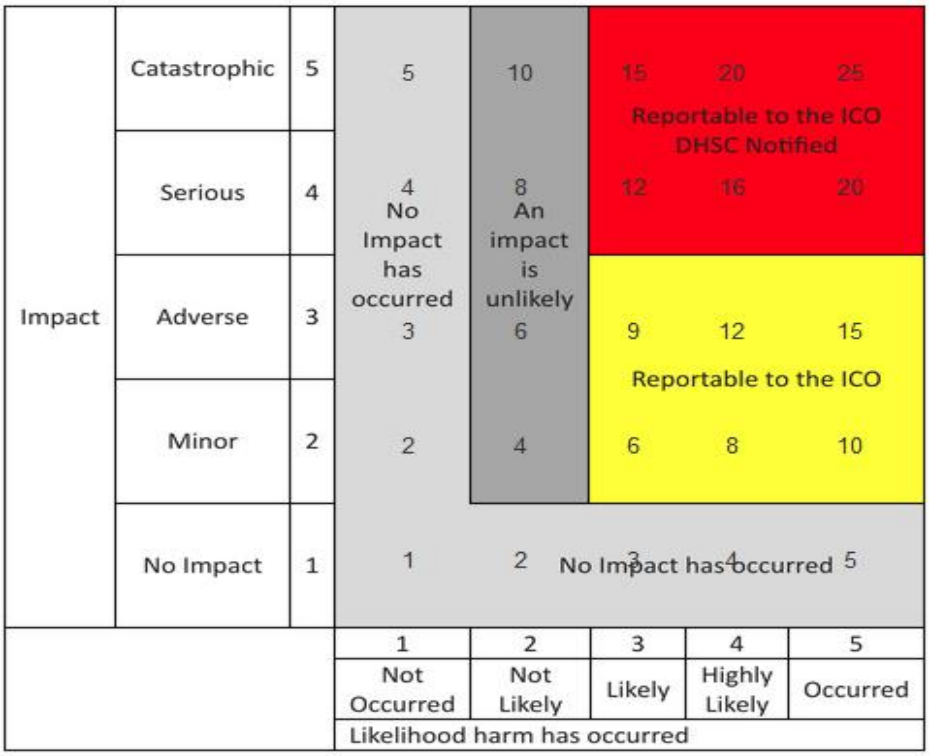
5.1 Breach Reporting to the ICO

All incidents must be graded according to the impact on the individual or groups of individuals and not the organisation. We use the following from NHS Digital's Guide to the Notification of Data Security and Protection Incidents to ascertain if an incident is reportable.

No.	Likelihood that	Description

	adverse effect has occurred	
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

No.	**Potential severity of the adverse effect on individuals**	**Description**
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence



If the breach includes special category data or involves vulnerable people the minimum level of likelihood and impact is a 2.

For all level 5 and above:
During office hours the Senior Information Risk Owner, Data Protection Officer and Information Governance Manager need to be informed of all notifiable data breaches. This can be done by email SIRO@hdft.nhs.uk, Dataprotectionofficer@hdft.nhs.uk and Information Governance Manager. Out of hours the Senior Manager on Call must also be informed.

Please include in the email:

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- a description of the likely consequences of the personal data breach
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

5.2 Unauthorised Access

Unauthorised access to information on patient system must be investigated by the Information Governance Manager or a deputy in their absence nominated by the Senior Information Risk Owner.

6 TRAINING

All substantive and bank staff receive data security training as part of their induction and receive annual refresher training.

Volunteers receive information governance training as part of their induction.

7 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has ultimate responsibility for compliance with the Data Protection Act 1998 and should ensure that

- responsibility for brining data protection issues for consideration by the senior level of management is delegated appropriately *(Senior Information Risk Officer)*
- a data protection lead or manager is in place to organise and enforce the approach to data protection and report directly to the above individual *(Data Protection Officer)*
- the role of the Caldicott Guardian is appropriately assigned and supported

Caldicott Guardian

The Caldicott Guardian:

- oversees the arrangements for the use and sharing of patient information
- plays a key role in ensuring the highest standards for handling patient identifiable information
- actively supports work to enable information sharing where appropriate to share
- advises on options for lawful an ethical processing the information
- represents and champions confidentiality and information sharing requirements and issues at senior management level

The Caldicott Guardian is required to be registered on the National Register of Caldicott Guardians.

Data and Information Governance Steering Group

The Data and Information Governance Steering Group has overall responsibility for overseeing the development and the implementation of information governance policies, procedures, audits and action plans. The DIGSG also reviews untoward occurrences and incidents relating to information governance and ensures that effective remedial and preventative action is taken. The Group also acts as the Caldicott Function. It is made up of Senior Information Risk Owner, Data Protection Officer, Information Governance Manager and Head of Patient Systems & Health Records. The DIGSG is also responsible with producing a Bi annual report to the Board of Directors containing the Data Security and Protection Toolkit results and highlighting associated issues.

The Caldicott Guardian

The Caldicott Guardian:

- oversees the arrangements for the use and sharing of patient information
- plays a key role in ensuring the highest standards for handling patient identifiable information

- actively supports work to enable information sharing where appropriate to share
- advises on options for lawful an ethical processing the information
- represents and champions confidentiality and information sharing requirements and issues at senior management level

Senior Information Risk Owner
The Trust's Senior Information Risk Officer (SIRO) is the Chief Operating Officer. The SIRO:

- takes overall ownership of the Organisation's Information Risk Policy
- acts as champion for information risk on the Board of Directors
- implements and leads the NHS information governance risk assessment and management processes within the Organisation
- advises the Board of Directors on the effectiveness of information risk management across the Organisation

Data Protection Officer
The Data Protection Officer is responsible for: informing and advising us and its employees about their obligations to comply with data protection laws; monitoring compliance with data protection laws; and being the point of contact regarding data protection.

Information Governance Manager
The Information Governance Manager is responsible for managing the organisations Information Governance function, including setting and implementing appropriate policies and procedures as well as ensuring appropriate audits and monitoring mechanisms are undertaken. The Information Governance Manger is responsible for initially reviewing information governance risks and escalating them DIGSG and the SIRO.

Information Governance Officer
The Information Governance Officer provides support to the Information Governance Manager. The Information Governance Officer ensures appropriate responses to all subject access requests in relation to patient information within the allocated timescale, liaising with the appropriate healthcare professionals.

Information Security Officer
The Information Security Officer Is responsible for providing advice on all aspects of information security and risk management. The quality of their assessment of information security risks, threats and advice on controls will contribute significantly to the effectiveness of the organisation's information security.

Unit/Department Managers
Unit/department managers are responsible for data protection practice within their work area ensuring:

- the working practices carried out within the unit/department are in line with the Trust's policies
- all staff within the work area are adequately trained and aware of their personal responsibilities for data protection issues

Information Asset Owners and Information Asset Administrators

Information Asset Owners will provide assurance that information risk is being managed effectively for their assigned assets. The Information Asset Owners will be supported by the Information Asset Administrators.

All staff

All employees are required to:

- Ensure that they are following all Trust Policies and Procedures and legislation outlined in section 2.
- Maintain the confidentiality of information about the Trust, its staff and its patients in accordance with the Trust's Information Governance policies and data protection legislation, during and after the termination of employment.
- Only access confidential information that they are required to do so as part of their role.
- Implement the appropriate technical and physical measures to ensure that confidential information is safe and secure.
- Familiarise themselves with the Trust's Information Governance policies and data protection legislation.
- Undertake Information Governance training on an annual basis.

Failure to comply with or adhere to the Trust's Information Governance Policies or data protection legislation will be treated as misconduct under the Trust's Disciplinary Policy, which may result in dismissal or criminal proceedings. The Trust's Information Governance Policies are available on the Trust's intranet page.

As an individual, you do have the right to apply to view or have copies of your own records via the appropriate routes. You do not have the right to directly access your own records. Inappropriate access to confidential information will be treated as misconduct under the Trust's Disciplinary Policy which may result in dismissal and/or criminal proceedings.

8 POLICY DEVELOPMENT

The stakeholders of this policy are all staff employed or contracted and voluntary staff.

9 CONSULTATION, APPROVAL AND RATIFICATION PROCESS

The consultation process undertaken at current document review is documented in Appendix 1. This document will be approved and ratified by the Data and Information Governance Steering Group.

10 DOCUMENT CONTROL

This document will be available on the Trust Intranet for read only access. As the document replaces a previous version, the old document will be archived within the

intranet. The front page of the document will indicate the version number, the approving body and the date of approval, along with the next review date.

Copies of this document should not be printed unless it is absolutely necessary, as there is a risk that out of date copies may be in circulation.

Requests for this document in an alternative language or format (such as Braille, audiotape, large print etc.) will be considered and obtained whenever possible.

11 DISSEMINATION AND IMPLEMENTATION

A “publish and point” method of communication will be used, where relevant staff are informed about the publication of a new or revised document on the intranet.

12 MONITORING COMPLIANCE AND EFFECTIVENESS

The Trust will monitor this Policy through the Data Security and Protection Toolkit. An assessment of compliance with requirements, within the Data Security and Protection Toolkit will be undertaken each year. Annual reports and proposed action/development plans will be presented to the Trust Board for approval prior to submission to the toolkit. It is assumed that both Internal and External Audit will review this and associated procedures.

An annual Information Governance Report will be submitted to the Data and Information Governance Steering Group.

All information governance incidents are reviewed and scored by the Data and Information Governance Steering Group.

Managers will also monitor compliance within their work area, and take appropriate action when infringements of this policy are brought to their attention.

13 REFERENCE DOCUMENTS

- Caldicott Principles
- Data Protection Act 2018
- General Data Protection Regulations 2016
- Care Records Guarantee
- NHS Code of Practice on Confidentiality
- NHS Code of Practice on Information Security Management
- Guide to Confidentiality in Health and Social Care
- The Health and Social Care (Safety and Quality) Act 2015
- NHS Constitution for England
- NHS Standard Contract
- NICE Clinical Guideline 138
- Quality Standard 15

- Quality Standard 15, Quality Statement 12
- Quality Standard 15, Quality Statement 13
- Human Rights Act 1998
- Statistics and Registration Service Act 2007
- Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation
- Cabinet Office: Data Handling Procedures in Government: Final Report
- Department of Health: Information Security Management NHS Code of Practice
- Department of Health: NHS Information Risk Management - Good Practice Guide
- NHS Digital: Guide to the Notification of Data Security and Protection Incidents

14 ASSOCIATED DOCUMENTATION

- Safeguarding Documents
- Police Policy.
- Information Sharing Protocol Template
- Information Sharing Agreement Template
- Fax Cover Template
- Guidelines for Sending Secure Faxes
- Pseudonymisation & Anonymisation of Data Policy
- Information Risk Management Policy
- Risk Management Policy
- Risk Register Template
- IT Clinical Safety Policy
- Identification, Reporting and Management of Incidents Including SUIs
- Information Security Risk Assessment and Management Strategy
- Data Protection Impact Assessment Template

15 APPENDICES

Appendix 1: Consultation Summary

Appendix 1: Consultation Summary

Those listed opposite have been consulted and any comments/actions incorporated as appropriate. The author must ensure that relevant individuals/groups have been involved in consultation as required prior to this document being submitted for approval.	**List Groups and/or Individuals Consulted**
	Data Protection Officer
	Senior Information Risk Officer
	Data and Information Governance Steering Group