Epsom and St Helier University Hospitals NHS Trust

INFORMATION GOVERNANCE POLICY

Ratified by:	Trust Executive Committee
Date ratified:	18 February 2020
Name of originator/policy author:	Paul Kenny
Name of responsible committee/individual:	Trust Executive Trust
Date issued:	February 2020
Review date:	September 2022
Target audience:	All Staff, Volunteers and Contractors
History:	Reviewed and updated August 2019

AMENDMENTS (No more than three per policy version)	DATE

Index

Contents

1. INTRODUCTION

The Epsom and St Helier University Hospitals NHS Trust (ESTH) recognise 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 (IG) plays a key part in supporting Clinical Governance, service planning and performance management. It also gives assurance to Trust staff 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.

This policy provides a framework for the overlapping areas of confidentiality and data protection compliance, freedom of information, information security (based on the Data Protection and Security Toolkit (DSPT) and data quality.

Information Governance aims to strike the right balance between:

- 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

Information Governance is owned by the Trust's most senior management. This is demonstrated by annually signing a Statement of Compliance via the Data Protection and Security Toolkit (DSPT) in respect to the Trust and any contracted services.

The Trust is registered with the Information Commissioner's Office as a Data Controller and processor of information, and must comply with its duties as set out in the data protection act.

A Non-Executive Director has been given responsibility for oversight of the Information Governance agenda.

IG Compliance is supported by the key roles of Caldicott Guardian, Senior Information Risk Officer (SIRO), Information Governance manager and data protection officer. However, all staff have a duty to ensure the security and confidentiality of personal information

2. SCOPE OF THE POLICY

This information governance policy is an overarching policy which sets out the principles of information governance which are intended to provide a consistent approach to:

- Establishing and maintain the security, quality and confidentiality of information, information systems, applications and networks owned or held by the Trust.
- 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.
- Ensue the Trust complies with relevant legislation and guidance.

This policy cannot be read in isolation as information plays a key part in corporate governance, strategic risk management, clinical governance, service planning, records management, freedom of information and performance management.

3. KEY AUDIENCE

All staff, Trust wide, whether permanent, temporary, volunteers or contracted must be aware of this policy and its content. The policy also applies to those providing services to or on behalf of the Trust

Every employee, volunteer, contractor and others providing services for or on behalf of the Trust will come into contact with sensitive information during some or all of their work for the Trust.

4. ROLES AND RESPONSIBILITIES

Board Responsibility

It is the role of the Trust Board to define the organisation's policy in respect of Information Governance, taking into account the legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy.

The Chief Executive

The Chief Executive is the accountable officer.

Senior Information Risk Officer (SIRO)

The SIRO has ultimate responsibility for the management and mitigation of risks associated with the Trust's information management processes. The SIRO is the chair of the Information Governance Committee.

The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the board.
The SIRO will act as an advocate for information risk on the board and in internal discussions and will provide written advice to the Accountable Officer on the management of information risk.

The key responsibilities of the SIRO are to:

1. Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.

2. Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.

3. Review and agree action in respect of identified information risks.

4. Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

5. Provide a focal point for the resolution and/or discussion of information risk issues.

6. Ensure the Board is adequately briefed on information risk issues.

7. Ensure that all care systems information assets have an assigned Information Asset Owner.

Caldicott Guardian

The Caldicott Guardian has a strategic role and is also responsible for promoting and ensuring that Caldicott principles are followed and that sharing of patient information is facilitated as appropriate.

To facilitate this, the Caldicott Guardian must maintain a strong knowledge of confidentiality and data protection and provide input to relevant Trust strategies, policies and procedures.

The Caldicott Guardian oversees all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows

of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.

Caldicott Guardians must be registered with the UK Caldicott Guardian Council. The register is maintained by NHS Digital.

Data Protection Officer (DPO)

The DPO provides the organisation with independent risk-based advice to support its decision-making regarding the appropriateness of processing personal and special categories of data within the principles and data subject rights as laid down in the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The DPO has oversight of investigations and reports to the ICO all breaches within 72 hours.

The DPO Provides advice on the completion of data privacy impact assessments (DPIA's) and whether a DPIA is required for the given processing.

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

The Data protection officer is responsible for overseeing the data protection strategy and implementation to ensure compliance with legislatory requirements.

The DPO Is independent and as set out in the data protection act cannot be instructed as to the content of the advice given.

The role of DPO may be carried out by one person or the role can be combined with another person's role.

The Trust is required to have a DPO.

Information Governance Manager

The information governance manager is a senior member of staff whose role includes:

- Providing management leadership for information governance and having responsibility for leading the strategic development of policies, procedures and standards relating to information governance.
- Providing specialist knowledge.
- Raises awareness and acceptance of information governance standards, with the aim of enabling information into the organisation.
- Working closely with the SIRO and Caldicott Guardian.

- Investigating or advising on Information Governance security issues including breaches and other information governance incident reports

- Ensuring that that the Trust's activities consistently support accountability, openness, fairness and transparency of process.

- Reviewing data flows for the release of personal identifiable information in conjunction with the Caldicott Guardian and SIRO.

- Being the first contact point for the information commissioner's office and citizens in terms of data processing.

- Ensuring that the Trust's business activities are conducted in a manner consistent with the data protection and Freedom of Information Act.

- To manage the Trusts Data protection and Security Toolkit submission.

- The information governance manager facilitates the provision of information governance training to Trust staff

Assistant Director of Performance and Information

Assistant Director of Business Intelligence ensures the application of relevant legislation, policy and procedure to the production of reports and other outputs produced by the performance and information team. The Assistant Director of Performance and information also provides analytical services to the Information Governance Committee and guidance to the Trust upon request.

Information Asset Owners (IAO)

Information asset owners are senior members of staff, usually a divisional general manager, who is the nominated owner for one or more identified information systems.

Information Asset Owners will support the organisations information governance goals and objectives by ensuring systems under their control or that they are responsible for, including cloud hosted systems, and the system users comply with current legislation and ensure the registration (completion of ICT standard operating procedure (SOP)) of the system is kept up to date and deposited with ICT as well as ensuring procedures are in place to achieve a high level of data quality.

Information Asset owners will provide at least annual reports as specified by the SIRO to the Trust information governance committee.

Information Asset Administrators (IAA)

The Information Asset Administrator's (IAA) primary role is to support the IAO to fulfil their responsibilities.

IAA's administer the systems they are responsible on a day to day basis ensuring for example user access rights are reviewed at least annually, users are added and removed promptly and ensuring that security and system patches are promptly applied.

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.

Managerial Accountability and Responsibility

All line managers within the Trust are responsible for ensuring that the policy and its supporting strategy, standards, procedures and guidelines are built into local processes and there is ongoing compliance.

Individual Responsibility (staff, volunteers, contractors permanent and temporary for example)

Every individual staff member, volunteer and contractor is responsible for ensuring they are aware of the requirements placed upon them and for ensuring they comply with these on a day to day basis.

Any staff member who does not comply with this policy, or breaches the confidentiality of patients/staff, will be subject to disciplinary procedures as per Trust policy, which may result in their dismissal, and if professionally registered, reported to their professional body.

5. THE INFORMATION GOVERNANCE COMMITTEE

Information Governance is managed through the Information Governance Committee which reports to the Patient Safety and Quality Committee. The committee normally meets on a quarterly basis.

The Information Governance Committee:-

- Ensures that all IG policies, including this policy, procedures and guidance are made available and are up to date
- Receives regular reports from information asset owners
- Receives regular data quality reports
- Receives reports regarding subject access requests (SARS) made under the Data protection Act and GDPR and requests made under the Freedom of Information Act
- Ensures corporate records are managed correctly
- Receives reports of incidents
- Reviews Data Privacy Impact Assessments (DPIA) for new systems or ways of working with person identifiable information
- Reviews the Trusts privacy notice and privacy materials

The information governance committee is chaired by the Senior Information Risk Owner.

6. TRUST ICT CHANGE CONTROL BOARD (CCB)

The Information Communications and Technology (ICT) Change Control Board meets weekly and reviews proposed new systems and changes to existing systems that process personal information or changes that may impact on the processing of personal information.

The CCB reports to the information governance committee.

The CCB is attended by core members drawn from Information communications Technology, Governance, Procurement and Clinical systems teams.

7. SUMMARY

A user friendly summary of Information Governance Do's and Don'ts is attached as appendix 1.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in the safety and effectiveness of clinical care, clinical governance, service planning and performance management. It is therefore of paramount importance to ensure that information is efficiently managed in accordance with legislation and guidance, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

This policy covers all aspects of information within the organisation, including but not limited to:

- Patient/Client/Service user information
- Staff related information
- Organisational information

The policy covers all aspects of handling information, including but not limited to:-

- Structured record systems (paper & electronic)
- Transmission of information (fax, email, post/courier & telephone).
- Fax machines should not be used except in an emergency.

The policy also covers all information systems purchased, developed and managed by the Trust and any individual (directly employed or otherwise by the Trust) accessing information 'owned' or 'managed' by the organisation.

The Trust regards all identifiable personal information as confidential except where national policy on accountability and openness or legislation requires otherwise.

Personal data can relate to information about patients, service users and members of staff or public that describes an identifiable person.

It does not have to include particular demographic information, such as name and address but can consist of a combination of factors that would make it possible to identify the person.

Information provided to the NHS and partner organisations, is done so on the expectation of confidentiality and often in a healthcare setting.
If personal data is also subject to a duty of confidentiality, for example because it relates to a patient, we refer to this as personal confidential data (PCD).
It is important for staff and working practice to take account for this and to ensure that any secondary use of personal confidential data that is for non-care purposes, is done in accordance with legal and organisational requirements including the national opt out.

As required by the data protection act the Trust must publish a privacy notice, which may be supplemented by divisional or departmental notices.

The privacy notice will be made available via various means including the Trust web site and leaflets for example as provided by the Patient Advice and Liaison Service (PALS).

The privacy notice sets out how the Trust uses and shared individual's information and what rights regarding their information individuals have.

Trust divisions must ensure patients are informed as to how their information will be used (processed), shared and what their rights regarding the processing are.

8. THE POLICY

This policy is based around the following 10 National Data Security Standards:

Leadership Obligation 1

> *People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles*

Data Security Standard 1

All staff must ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form.
Personal confidential data is shared for only lawful and appropriate purposes.

All staff managing change must ensure that they identify any potential information governance requirements when scoping the case for any change. Where new processing or a change to existing processing of personal data is to take place a data privacy impact assessment must be completed by the IAO and reviewed by the

information governance manager be being presented for signed off by the Caldicott Guardian and Senior Information Risk Owner.

The three four basic components of information security are:

- **Confidentiality**: assuring that sensitive information or data is accessible to only authorised individuals and is not disclosed to unauthorised individuals or the public.

- **Integrity**: safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.

- **Availability**: ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.

- **Accountability** – Users are held responsible for their use of information

See the Trust information security policy for further information.

Transfer of Information

All transfers of information within and outside the Trust must be managed, comply with the information security requirements and follow clear process.

All IAO's must have clearly documented their inward and outward flows of personal data and personal confidential data this will be achieved via the information flow mapping process. The recording template will be provided by the Trust information governance team.

Information flow mapping must be reviewed and updated annually.

IAO's must ensure staff use the correct method of transfer taking into account the sensitivity of the data.

Before personal patient information is processed for non-direct health care purposes (secondary use, planning and research) the patient wishes must be checked against the national opt out database.

Data Security Standard 2
All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3
All staff complete appropriate annual data security training and pass a mandatory test, provided through the Data Security and Protection Toolkit or through in-house training materials approved by the SIRIO.

Leadership Obligation 2

Process: Ensure the organisation proactively prevents data security breaches and respond appropriately to incidents or near misses

Data Security Standard 4
Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on ICT systems can be attributed to individuals.

Where possible use will be made of anonymised or pseudonymised, patient or staff, data.

Data Security Standard 5
Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security. This is part of the Trust's overall risk management arrangements and is described in detail in the Risk Management Policy suit.

Data Security Standard 6
Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7
A continuity plan is to be put in place to respond to threats to data security, including significant data breaches or near misses, and it is to be tested once a year as a minimum, with a report to the information governance committee.

Leadership Obligation 3

Technology: Ensure technology is secure and up-to-date.

Data Security Standard 8
No unsupported operating systems, software or internet browsers are used within the ICT estate.

All systems used to process Trust person identifiable information must be approved by the Trust Information, Communications and Technology change control board in writing.

Data Security Standard 9
A strategy is in place for protecting ICT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10
Information communications and technology suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Information Communications and Technology suppliers that process personal information must successfully annually complete the NHS Digital Data Protection and Security Toolkit (DSPT). It is the responsibility of the appropriate IAO to ensure that contracts, processing agreements and sharing agreements are put in place before processing takes place.

The Information security arrangements are described in detail in the sub policy ***Information Security Policy***.

The Data Protection Act

Principles relating to processing of personal data

The Trust (as a Data controller) is responsible for and must be able to demonstrate compliance with the Data Protection Act which incorporates the GDPR.

The data protection act sets out the data protection principles as below which must be adhered to:

Personal Data must be:

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

b. 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;

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

d. 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;

e. 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

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

Accountability is central to the data protection act. Data controllers (including the Trust) are responsible for compliance with the above principles and must be able to demonstrate compliance to data subjects and the regulator (The Information Commissioners Office (ICO))

It is a requirement of the DPA that data controllers (IAO's) record the legal basis for the processing of the personal data for which they are responsible and / or is processed within their division.

The record of the legal basis of processing must be reviewed / updated annually. A template for documenting the legal basis of processing is available from the information governance team.

IAO's must present their record of processing to the information governance committee annually.

Rights of the Data Subject

A data subject is any person whose personal data is being collected, held or processed.

Under the data protection act data subjects have the following rights.

The ability for a data subject to enforce certain of their rights may be limited in the health care environment such as the “right to be forgotten”.

- 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 the Trust carries out automated decision-making and profiling

If sending personal information outside the European Economic Area it is necessary to ensure the correct controls are in place to ensure the data is adequately protected.

See the Trusts privacy notice for further information.

Subject Access Requests

Data subjects can under the data protection act request copies of their information held by the Trust. Guidance on the process can be found on the Trust external web site.

For patients, access to health records falls under the Data protection Act 2018 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.

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 child's rights to confidentiality have to be balanced against parental responsibility).
- Patient representative – A person nominated to make healthcare decisions on behalf of the patient
- Executor of a will/Persons who may have a claim arising out of the patients estate

See the health records policy for further information and the Trust website.

Staff, volunteers and others the Trust holds information on also have the right to ask for information held by the Trust about them them resulting from their employment. Such requests should be sent to esth.staffsar@nhs.net

Confidentiality and Openness

The Trust regards all identifiable personal information relating to patients as confidential.

The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

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

Non-confidential information describing the Trust and its services will be available to the public through a variety of media. The Trust will have clear procedures and arrangements for handling queries from patients and the public. Particular consideration will be given to ensure that certain groups (e.g. people with visual impairment, people for whom English is not their first language) are not disadvantaged. This will be undertaken in line with the sub policy entitled: ***Freedom of Information Policy***.

Patients will have ready access to information relating to their own health care, including the records that health professionals have made about them (either on paper or on computers) their options for treatment and their rights as patients, in line with the sub policy entitled: ***Health Records Management Policy*.**

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media. This will be undertaken in line with the with the sub policy entitled: ***Media and filming Policy***

Information Security is the responsibility of all mangers and staff who must ensure they follow policies, guidelines, best practice and comply with the law.

Information security is managed through the Information Governance committee chaired by the SIRO supported by the Information Communications and Technology change control board.

The Trust will promote effective confidentiality and Information Communications and Technology security practices to its staff through policies, procedures and training.

The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential threats and breaches of confidentiality and security. Incidents must be recorded on the Datix incident reporting system.

Breaches of the Data Protection Act must be reported as quickly as possible to allow the Trust to report the incident to the regulator (Information Commissioner) within 72 continuous hours of the Trust becoming aware of the breach.

Please see the Information Governance page on the Trust intranet for further information including NHS Digital guidance on reporting. http://www.victor.epsom-sthelier.nhs.uk/information-governance

Non confidential information on the Trust and the services it provides should be available to the public by means of a request made under the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

The Trust will undertake or commission regular assessments and audits of its information security procedures and practices.

Data Quality

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

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records. This will be undertaken in line with the with the sub policy entitled: ***Health Records Management Policy***

Managers are expected to take ownership of, and seek to improve, the quality of information within their services. Wherever possible, information quality will be assured at the point of collection. Data standards will be set through clear and consistent definition of data items, in accordance with national standards. This will be undertaken in line with the sub policies entitled**:** ***Data Quality Policy*** and ***Clinical Coding Policy.***

The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.

Good quality data means that data is recorded in full, as accurately and in a timely manner as possible. Timely data entry will help avoid discrepancies and inaccuracies. Where it is not possible to enter data in real-time this data should be recorded as soon after the event as possible.

Data should not be duplicated unless absolutely necessary and this fact should be recorded with the original data. If duplicated the data owner must ensure that all copies of the data are kept up to date and synchronised.

Managers in general will take ownership of, and seek to improve, the quality of information within their services. Information Asset Owners will be designated for information assets. Divisional General Managers will be normally be designated IAO's although day to day responsibility may be formally delegated.

Availability

The Trust also recognises the utmost importance of having the right information available in the right place at the right time and the need to share patient information appropriately with those providing care. Information sharing with other healthcare partners will be in a controlled manner consistent with the interests of the patient, and, in some circumstances, the public interest.

Accuracy – staff must ensure that information is accurate

Completeness – the relevant information required is identified and working practice ensures it is routinely captured

Relevance – information is kept relevant to the issues rather than for convenience with appropriate management and structure.

Timeliness – information is recorded as close to possible to being gathered and can be accessed quickly and efficiently

Retention and Erasure

The Trust will comply with the NHS Records Management Code of Practice for Health and Social Care 2016 and any amendments thereto and related legislation. When the Trust no longer requires to retain personal information it will be erased / destroyed in accordance with Trust policy – including the ***Equipment and media disposal policy***

The Trust's Privacy notice which is available on the Trust web site https://www.epsom-sthelier.nhs.uk/your-information-and-what-you-should-know and from the PALS offices sets out the how the Trust processes personal data and how an individual may request erasure.

9. LEGAL AND REGULATORY FRAMEWORK

There is a long list of legal and regulatory instruments that are cited in this policy, which may not be exhaustive. The DSPT Toolkit provided by NHS Digital provides a practical orientation in the aspects of these instruments that have a bearing on the NHS. This Information Governance policy is set out to comply with the following national legislation and the NHS regulatory framework

10. LEGISLATION

The organisation is bound by the provisions of a number of items of legislation affecting the stewardship and control of information.
The main relevant legislative acts are:

- Data Protection Act / General Data Protection Regulation 2018 (and subsequent Special Information Notices)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 2018)
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Crime & Disorder Act 1998
- Electronic Communications Act 2000
- Mental Health Act 2007
- Protection of Children Act
- Police and Criminal Evidence Act 1984
- Common Law duty of confidentiality
- Health and Social Care Act 2012
- Public Records Act 1958, 1967 and 2005
- Health and Social care (Quality and Safety) Act 2015Children's Act 1989

In addition to the above, other legislation can impact upon the way in which the Trust will use information. This secondary legislation includes:

- Public Interest Disclosure Act 1998
- Audit & Internal Control Act 1987
- NHS Sexually Transmitted Disease Regulations 2000
- National Health Service Act 1977 / 2006
- Human Fertilisation & Embryology Act 1990 (disclosure of information)
- Abortion Regulations 1991
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992

- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health & Safety at Work Act 1974

Regulations

Caldicott Committee Report 2013
NHS Confidentiality Code of Practice 2003
DoH Records Management: Code of Practice 2016
NHS Digital – Data Security & Protection Toolkit – National Data Security Standards
Care Quality Commission Standards

11. NHS REGULATORY FRAMEWORK

In relation to many of the above requirements the NHS has set out and mandated a number of regulatory elements that now, taken together with the above national legislation, form the basis of 'Information Governance'.
This is an area of on-going development and evolvement.
The main regulatory elements are:

- Caldicott – Report, audit & improvement on the use of Patient Identifiable Data
- ISO1(BS)7799 – British Standard for Information Security Management, mandated for the NHS in 2001 and supported by the Data Security Protection Toolkit (DSPT)
- Records Management: NHS Code of Practice (2006)
- Confidentiality Code of Practice (2003)
- The Data Security Protection Toolkit (DSPT)

12. LEGAL COMPLIANCE

The following table shows how the legal documents are translated into Trust Policy.

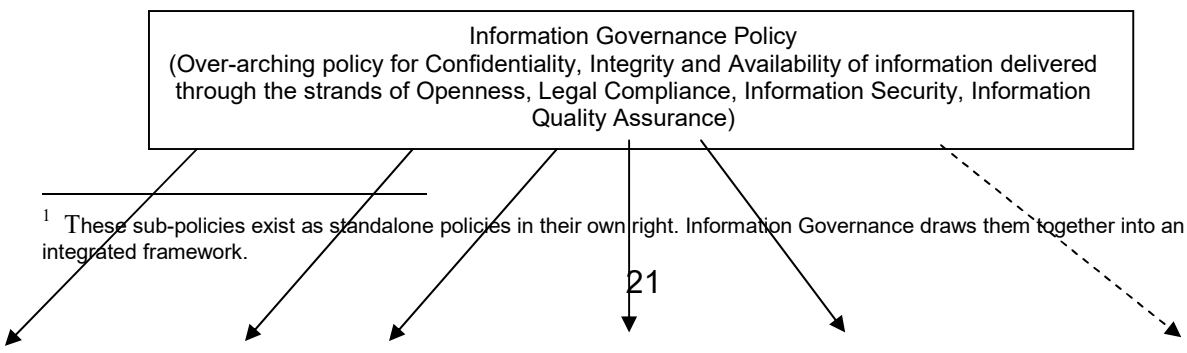
Law	**Related Trust Policy**
Data Protection Act / GDPR 2018 (and subsequent Special Information Notices)	Mainly represented in the *IS* ***Information Security Policy*** but the DPA also pervades every policy relating to IG.
Human Rights Act 1998	***IS Information Security Policy*** in relation to the way in which employee's use of email/internet etc can and cannot be monitored.

Freedom of Information Act 2000	***Freedom of Information Policy*** ***Health Records Management Policy***
Access to Health records act 1990	***Health Records Management Policy***
Computer Misuse Act 1990	***IS Information Security Policy*** - this policy contains statements on "acceptable use" of computing equipment and a "Do's and Don'ts section" Supported by the Trusts completion of the annual DSPT
Copyright, designs and patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992	As above
Electronic Communications Act 2000	As above
Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)	***IS Information Security Policy*** in relation to the way in which employees' use of email/internet etc can and cannot be monitored. In lay terms this law provides something of a counterbalance to the Human Rights Act.
Mental Health Act 2007	
Protection of Children Act	

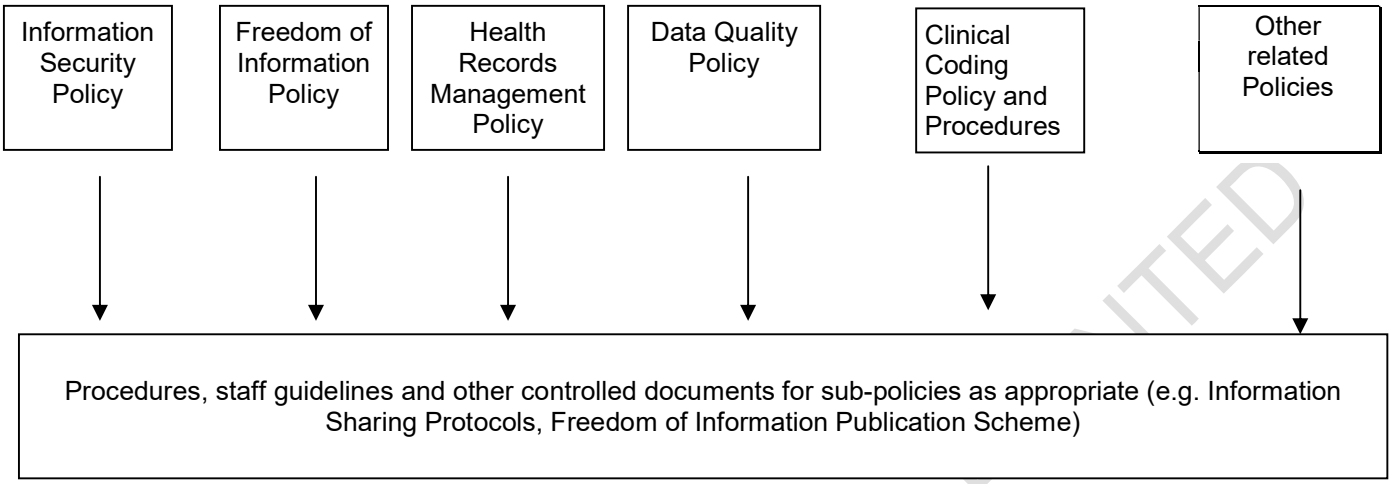
The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.

13. OVERALL POLICY STRUCTURE

The Information Governance Policy and the principles which drive it set the high-level direction and required standards across the Trust. As shown in the structure below, these will be supported where necessary by specific sub-policies[1], where the relevant information governance requirements will be set out in detail. Underpinning most of these sub-policies will be the detailed procedures and guidelines to which Trust staff will be expected to adhere. They are easily accessible to all staff on the Trust's intranet.



[1] These sub-policies exist as standalone policies in their own right. Information Governance draws them together into an integrated framework.



14. TRAINING AND AWARENESS

Information Governance training is a yearly mandatory requirement for all staff, volunteers or others with access to Trust person identifiable data and business information.

Managers must ensure the appropriate training modules as sign posted by the Senior Information Risk Owner are undertaken by staff, volunteers and others with access to person identifiable data and business information.

Some roles require extra training such as the Data Protection Officer; SIRO, Caldicott Guardian, Information team, medical records staff and Communications and Technology Security Specialists (this is not an exhaustive list)

The Trust provides information governance training at Trust induction and runs mandated Information Governance training sessions for all staff and volunteers.

Important or new Information Governance issues and information are to be communicated via various Trust communication channels including the intranet and electronic news letters.

Information and documents relating to Information Governance will be made available on the Trust's Intranet site.

Compliance with the mandatory annual training will be included in all services Performance Dashboards, and monitored at Divisional Performance Reviews and at the Information Governance Committee.

15. MONITORING & REVIEW

This policies effectiveness will be reviewed by the information governance committee through the monitoring of reported incidents relating to breaches of confidentiality, and loss of personal information.

In line with the Data Security and Protection Toolkit annual staff surveys will be undertaken to provide the Trust awareness of training effectiveness.

The Information Governance Committee will ensure that this policy is kept up to date by checking on an annual basis that it remains current and a full review will be carried out three years after publication.

16. REFERENCES

Access to Health Records Act 1990, c. 23, [online] Available at: http://www.legislation.gov.uk/ukpga/1990/23/contents (Accessed 30 January 2020).

Computer Misuse Act 1990, c. 18, [online] Available at: http://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed 30 January 2020).

Copyright, Designs and Patents Act 1988, c. 48, [online] Available at: http://www.legislation.gov.uk/ukpga/1988/48/contents (Accessed 30 January 2020).

Crime and Disorder Act 1998, c. 37, [online] Available at: http://www.legislation.gov.uk/ukpga/1998/37/contents (Accessed 30 January 2020).

Data Protection Act 2018, c. 12, [online] Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed 28 January 2020).

Electronic Communications Act 2000, c. 7, [online] Available at: http://www.legislation.gov.uk/ukpga/2000/7/contents (Accessed 30 January 2020).

Freedom of Information Act, 2000, c. 36, [online] Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents (Accessed 30 January 2020).

Health and Social Care Act 2012, c. 7, [online] Available at: http://www.legislation.gov.uk/ukpga/2012/7/contents (Accessed 30 January 2020).

Human Fertilisation and Embryology Act 1990, c. 37, [online] Available at: http://www.legislation.gov.uk/ukpga/1990/37/contents (Accessed 30 January 2020).

Human Fertilisation and Embryology Act 2008, c. 22, [online] Available at: http://www.legislation.gov.uk/ukpga/2008/22/contents (Accessed 30 January 2020).

Human Rights Act 1998, c. 42, [online] Available at: http://www.legislation.gov.uk/ukpga/1998/42/contents (Accessed 30 January 2020).

Mental Health Act 2007, c. 12, [online] Available at: http://www.legislation.gov.uk/ukpga/2007/12/contents (Accessed 30 January 2020).

Anon (1984) Police and Criminal Evidence Act 1984, c. 60, [online] Available at: http://www.legislation.gov.uk/ukpga/1984/60/contents.

Prevention of Terrorism (Temporary Provisions) Act 1989 (Continuance) Order 2000, No. 835, [online] Available at: http://www.legislation.gov.uk/uksi/2000/835/contents/made (Accessed 30 January 2020).

Protection of Children Act 1999, c. 14, [online] Available at: http://www.legislation.gov.uk/ukpga/1999/14/contents (Accessed 30 January 2020).

Public Interest Disclosure Act 1998, c. 23, [online] Available at: http://www.legislation.gov.uk/ukpga/1998/23/contents (Accessed 31 January 2020).

Public Records Act 1958, c. 51 (Regnal. 6_and_7_Eliz_2), [online] Available at: http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51/contents (Accessed 31 January 2020).

Public Records Act 1967, c. 44, [online] Available at: http://www.legislation.gov.uk/ukpga/1967/44/contents.

Regulation of Investigatory Powers Act 2000, c. 23, [online] Available at: http://www.legislation.gov.uk/ukpga/2000/23/contents (Accessed 31 January 2020).

Road Traffic Act 1988, c. 52, [online] Available at: http://www.legislation.gov.uk/ukpga/1988/52/contents (Accessed 30 January 2020).

The Abortion Regulations 1991, No. 499, [online] Available at: http://www.legislation.gov.uk/uksi/1991/499/contents/made (Accessed 30 January 2020).

The Children Act 1989 (Amendment) (Children's Services Planning) Order 1996, No. 785, [online] Available at: http://www.legislation.gov.uk/uksi/1996/785/contents/made (Accessed 30 January 2020).

The Copyright (Computer Programs) Regulations 1992, No. 3233, [online] Available at: http://www.legislation.gov.uk/uksi/1992/3233/contents/made (Accessed 30 January 2020).

The Health and Social Care (Safety and Quality) Act 2015 (Commencement No. 2) Regulations 2016, No. 906 (C. 63), [online] Available at: http://www.legislation.gov.uk/uksi/2016/906/contents/made (Accessed 30 January 2020).

The National Health Service (Venereal Diseases) Regulations 1974, No. 29, [online] Available at: http://www.legislation.gov.uk/uksi/1974/29/contents/made (Accessed 30 January 2020).

The National Health Service (Venereal Diseases) Regulations 1974, No. 29, [online] Available at: http://www.legislation.gov.uk/uksi/1974/29/contents/made.
British Standards Institution (2013) *Information technology. Security techniques. Information security management systems. Requirements (BS EN ISO/IEC 27001:2017)*, British Standards Institution.

Care Quality Commission (2014) Our fundamental standards, [online] Available at: https://www.cqc.org.uk/news/stories/our-fundamental-standards (Accessed 30 January 2020).

Epsom and St Helier University Hospitals NHS Trust (2020) Information Governance, *Victor: Epsom amd St Helier Intranet pages*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/information-governance (Accessed 30 January 2020).

Epsom and St Helier University Hospitals NHS Trust (2016) Pseudonymisation and Anonymisation Policy ESH/POL/32816, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n8348&ver=25658 (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2019a) Clinical Coding Policy ESH/POL/32716, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7356&ver=25749 (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2015) Data Quality Policy ESH/POL/30215, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7368&ver=17924 (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2018a) Freedom of Information Policy ESH/POL/47018, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7402&ver=25652%0A (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2018b) Health Records Management Policy ESH/POL/45318, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7417&ver=21521%0A (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2016) Information Security Policy ESH/POL/36716, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7423&ver=25669%0A (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2014) IT Equipment and Media Disposal Policy ESH/POL/14214, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7515&ver=25671 (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2019b) Media and Filming Policy ESH/POl/51619, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n10205&ver=25655 (Accessed 29 January 2020).

Epsom St Helier University Hospitals NHS Trust (2011) Mobile Telephone Policy ESH/POL/02011, *Victor: policies and guidelines*, [online] Available at: http://www.victor.epsom-sthelier.nhs.uk/download.cfm?doc=docm93jijm4n7556&ver=25673 (Accessed 29 January 2020).

Information Commissioners Office (2020) Information Commissioners Office, [online] Available at: https://ico.org.uk/ (Accessed 29 January 2020).

Information Governance Alliance (2016) Records Management Code of Practice for Health and Social Care 2016, [online] Available at: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/n/b/records-management-cop-hsc-2016.pdf (Accessed 30 January 2020).

NHS Digital (2020) Data Security and Protection Toolkit, [online] Available at: https://www.dsptoolkit.nhs.uk/ (Accessed 30 January 2020).

NHS Digital (2018) Data Security Standards: Overall guide. The bigger picture of where the standards fit in, [online] Available at: https://www.dsptoolkit.nhs.uk/Help/Attachment/126 (Accessed 30 January 2020).

NHS Digital (2019) National data opt-out, [online] Available at: https://digital.nhs.uk/services/national-data-opt-out (Accessed 29 January 2020).

NHS Digital (2016) Records Management Code of Practice for Health and Social Care 2016, [online] Available at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016 (Accessed 29 January 2020).

United Kingdom: Department of Health (2003) Confidentiality: NHS Code of Practice,

[online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf (Accessed 29 January 2020).

United Kingdom: Department of Health (2013) Information Governance Toolkit: Caldicott Principles, [online] Available at: https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx (Accessed 30 January 2020).

United Kingdom: Department of Health (2000) NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000, [online] Available at: https://webarchive.nationalarchives.gov.uk/20130123190356/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsLegislation/DH_4083027 (Accessed 30 January 2020).

Appendix 1

In the Office

•Remember to lock and secure the office when it is unattended and at the end of the day

•Whenever possible, escort visitors at all times
Sign-in visitors at Security for temporary ID

•Remember always to wear your Trust ID

•Do not write / store door codes on the back of your ID or attach keys to the lanyard.

On the Telephone

- Do you have a procedure for leaving messages on answerphones?
- Do you have a procedure for securely taking messages from the answerphone?
- Can the message be overheard?
- When receiving calls requesting personal information:
  - Verify the ID of the caller.
  - DO NOT ask if the date of birth is XX/YY/ZZ or if their address is "3 Never Street". Ask the patient or carer to TELL YOU their details - DO NOT provide the details to the caller
  - Ask for a reason for the request
  - If in doubt as to whether information should be disclosed, tell the caller you will call them back while you seek advice from your manager.

When providing personal confidential information, be alert to Child and Adult safeguarding issues - someone may want to know where a child is living in order to harm them.

Your Computer

•Ensure your PC or terminal is located where the screen cannot been seen by visitors or staff who are not authorised to access the information on screen – if need be, special filters can be fitted
•Always keep your password confidential, do not write it down
•Never share passwords – this is a disciplinary offence
•Change your password regularly – Trust systems will prompt this
•Always log off or use password protected screen savers if you leave your workstation.
•Only use Trust encrypted removable media such as memory sticks

Faxing – *Fax Only in Emergencies*

- Do not fax personal or confidential information unless absolutely necessary
- Always ensure you only send faxes to the recipient's "Safe haven" fax
- If you are faxing, always:
  - Double check the fax number and Fax a cover page.
  - Confirm receipt of the cover page.
  - Then immediately fax the data using the fax machines redial button.
  - Mark the fax 'Private & Confidential'.
  - Use the Trust fax template.
- For receiving faxes, please only use the Trust's "Safe Haven" fax numbers.

<table>
<tr><td></td><td>

- **Contact ICT regarding alternatives to using Fax machines.**

</td></tr>
<tr><td>

Email

Patient information should not, if possible, be sent via standard email. If it is necessary, it must be encrypted and sent care of an NHSnet contact – i.e. the sender and recipient must have a name@nhs.net email account or the [secure] service is used (see NHSmail help).

Some additional email systems have been declared secure by NHS Digital. Details can be found in the NHS mail help tool and on the information governance page on Victor.

</td><td>

Laptops, 'Phones and Tablets

- Confidential information should not normally be taken off any Trust site without authorisation
- When it is absolutely necessary, do remember:
  - Never leave a laptop / device unattended
  - Never leave a laptop / device in view on a car seat
  - Ensure regular housekeeping of laptops, delete old files and documents
  - Use encryption software to protect files containing confidential information
  - Ensure your laptop screen cannot be seen by others

Only use Trust encrypted removable media such as memory sticks

</td></tr>
<tr><td>

Photocopying

- Do not make excessive copies of confidential information
- Regularly check/update distribution lists to ensure unnecessary copies are not circulated
- Shred any unwanted copies or place in confidential waste bins, do NOT throw them into the ordinary bin

</td><td>

Printers

- Do not print confidential/personal information to shared/central printers without "follow me" security
- Keep the number of copies to a minimum
- Shred any unwanted copies or place in confidential waste bins, do NOT throw them into the bin

</td></tr>
<tr><td>

Filing Cabinets

- Keep filing cabinets locked at all times – not just at the end of the day
- Consider carefully where filing cabinets are located, and where you keep the keys
- Do you have procedures for house keeping – are you aware of the NHS retention guidelines?

</td><td>

POST

- Choose the most appropriate method of posting, eg Special Delivery, Data Post, etc.
- Ensure envelopes and packages are marked 'Private and Confidential'
- Double check the recipient's address
- Consider adding the sender's address – depending on sensitivity.
- Is the envelope strong and the package securely sealed?

</td></tr>
<tr><td></td><td></td></tr>
</table>

Appendix 1

Bins • NEVER place confidential waste in the domestic or clinical waste bins • Place any unwanted copies in the confidential waste bins.	***Personal*** • Hold confidential conversations in an appropriate place – not in the corridor, lift or the restaurant for example. • THINK very carefully where you use your mobile phone! • When you play back answerphone messages make sure they can't be over heard.
Any Queries? **Contact the ICT Help Desk on extension 2333**	