Essex Partnership University
NHS Foundation Trust

INFORMATION GOVERNANCE AND SECURITY POLICY

POLICY REFERENCE NUMBER:	CP50
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	3 year review
AUTHOR:	[redacted] Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Sub-Committee. Quality Committee.
IMPLEMENTATION DATE	May 2018
AMENDMENT DATE(S)	Feb 2018; May 18 (GDPR); May 2021
LAST REVIEW DATE	May 2021
NEXT REVIEW DATE	May 2024
APPROVAL BY IGSSC	April 2021
RATIFIED BY QUALITY COMMITTEE	May 2021
COPYRIGHT	

PROCEDURE SUMMARY		
The purpose of this procedural guideline is to establish the governance arrangements and responsibilities for information security, with the intention to promote and build a level of consistency across the Essex Partnership University NHS Foundation Trust ('the Trust') to safeguard information, ensuring all Trust staff are aware of their individual responsibilities.		
The Trust monitors the implementation of and compliance with this procedure in the following ways:		
The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate. Also through Trust Datix Reporting and Compliance with the IG Data Security & Protection Toolkit submission		
Services	**Applicable**	**Comments**
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is The Executive Chief Finance & Resources Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION GOVERNANCE AND SECURITY POLICY

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Information Governance and Security Policy

1.0 INTRODUCTION

1.1 The information used by the Trust is a vital business asset in terms of both clinical management of patients and the efficient management of services and resources. Protecting its confidentiality, integrity and availability is essential in preserving the Trust's reputation, efficiency, and its ability to comply with legal obligations.

1.2 Information / data has a key role in clinical and corporate governance, service planning and performance management.

1.3 Information governance deals with the way an NHS Trust handles personal, confidential and sensitive information / data about patients and staff and allows organisation and individuals to ensure that such information is dealt with in line with legislation, securely, efficiently and effectively.

1.4 Information governance will form the framework that merges all of the standards and best practice that apply to handling of person identifiable information / data.

1.5 It is vital therefore, that information / data is efficiently managed and that the appropriate policies and procedures are in place with management accountability and structures to provide a robust governance framework for information / data management.

1.6 To function effectively, ethically and legally the Trust needs to work within a framework of agreed rules.

1.7 This document sets out the Trust's intent for the safe and legal use of the facilities / systems provided by the Trust.

1.8 This policy and its associated procedures should be read in conjunction with other national guidance, Trust policies and other relevant legislation, including:

- Information Quality Assurance
- British Standard for Information Security ISO/IEC27000 series
- NHS Caldicott Report Recommendations
- The National Health Service Act (2006)
- Data Protection Act (2018)
- General Data Protection Regulation
- Access to Health Records Act (1990) (Where not superseded by the Data Protection Act (2018))
- Freedom of Information Act (2000) (FOI) (including Publication Scheme)
- The Environmental Information Regulations (2004) (EIR)
- Computer Misuse Act (1990)

- Electronic Communications Act (2000)
- The Re-Use of Public Sector Information Regulations (2005)
- The Civil Contingencies Act (2004)
- The Human Rights Act (2000)
- The Copyright, Designs and Patents Act (1988) (as amended by the Copyright Computer Programs Regulations (1992))
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- Crime and Disorder Act (1998)
- Health and Social Care Act (2000)
- The Common Law Duty of Confidentiality
- Integrated Governance Strategy
- Information Governance Framework
- Records Strategy
- IM&T Security Policy
- Data Protection and Confidentiality Policy / Procedure
- Freedom of Information Policy / Procedure
- Records Management Policy and related Procedures
- Mobile Working and Remote Access Policy/Procedures
- Data Quality Policy
- Virtual Private Network Policy
- Closed Circuit Television (CCTV) Policy / Procedure
- Information Governance and Security Procedures
- Paper and Electronic Corporate Records (Laserfiche) Policy / Procedures
- IT&T Security Procedures
- Internet/Email Access and Use Procedures
- Information Sharing & Consent Policy / Procedure
- ***This list is not exhaustive***...

1.9 There are many different types of legislation which relate to Information Governance, some are listed above but there is a full list in the Department of Health NHS Information Governance Guidance to Legal and Professional obligations

2.0 DUTIES / RESPONSIBILITIES

2.1 For the purposes of this policy, the definition of all staff includes all personnel working for or with the Trust, or who have been authorised to access the Trust's information assets. This includes all management, permanent employees, contractors, temporary staff, bank staff, locum, consultants, and agents/agency employees (***this list is not exhaustive***).

2.2 All employees of the Trust, permanent employees, contractors, temporary staff, bank staff, locum, consultants, and agents/agency employees (***this list is not exhaustive***) are required to abide by the contents of this policy and its associated procedural guidelines. Failure to do so may result in disciplinary action.

Responsible Persons

2.3 **Overall Responsibility Chief Executive**

2.3.1 The Chief Executive has overall responsibility as accountable officer for the management and implementation of information governance / security for the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

2.3.2 As such the Chief Executive Officer signs up to the 'Statement of Compliance' declaration agreeing with its strict terms and conditions in relation to the security requirements for using N3 and for access to the Internet and NHS Connecting for Health applications.

2.4 **Senior Information Risk Owner (SIRO).**

2.4.1 The Chief Executive has delegated the day to day responsibility for information governance / security, policy and implementation to the Executive Chief Finance Officer as the Trust's Senior Information Risk Owner (SIRO).

2.4.2 Making arrangements for information governance / security by setting / agreeing the overall policy for the Trust taking into account legal and NHS requirements.

- Appointing the Information Governance Security Manager / key leads.
- Appointing a Data Protection Officer to ensure that the provision of the Data Protection Act / GDPR is satisfied.
- Ensuring that, where appropriate, staff receive information governance / security awareness and training
- Chairing the Information Governance Steering Sub-Committee on a regular basis and through the Committee maintaining the Trust's Information Governance / Security risk register and escalating any related risks to the Quality Committee

2.5 **Caldicott Guardian**

2.5.1 The Chief Executive has delegated responsibility for Caldicott issues to the Executive Medical Director, who is the Caldicott Guardian. The Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of their person identifiable information / data, together with ensuring that patient identifiable information / data is shared in an appropriate and secure manner.

2.5.2 The Trust has dedicated forums for the monitoring of Caldicott Principles through the:

- Clinical Governance & Quality Committee
- Information Governance Steering Sub-Committee
- Caldicott Network

who are responsible for:

- Developing local protocols governing the disclosure of patient information to other organisations.
- Performing regular reviews and justifying the uses of patient information.
- Establishing access control policies for patient identifiable information.
- Improving organisational performance.
- Approving major initiative to enhance information governance / security.
- Reviewing and monitoring security incidents and compliance to this policy and its associated procedures.
- Monitoring significant changes in the exposure of information assets to major threats.

2.6 Information Governance Manager

2.6.1 The Information Governance Manager and / or Information Governance Administrators will oversee the day to day information governance issues and is responsible for:

- Working closely with the Trust's key information governance / security leads to ensure the actions below are implemented:
- Acting as a central point of contact on information governance / security within the Trust, for both staff and external organisations.
- Co-ordinating all Information Governance initiatives and producing the annual improvement plan / work programme
- Providing operational support for legal requirements, e.g. General Data Protection Regulation Data Protection Act (2018) and Freedom of Information Act (2000) compliance
- Assisting in the formulation of any information governance / security related policies and procedures and monitoring of compliance
- Producing Trust standards, procedures and guidance on information governance / security matters for approval by the Executive Team and / or Trust Board
- Co-ordinating breaches in information governance / security, ensuring the appropriate Security Incident Forms are completed for each breach, and assessing the nature of such incidences, carrying out investigations where appropriate and considering what recommendations can be made
- All information Governance related activities.
- Agreeing and supporting organisation-wide information security initiatives, e.g. information security awareness programmes.

- Promoting and supporting the development of information security standards and procedures related to information governance.
- Attending the Information Governance Steering Sub-Committee a regular basis and through the Committee maintaining the Trust's Information Governance risk register
- The Information Governance Team is responsible for the definition, implementation and monitoring of the Information Asset Management System (IAMS) and Data Flow Mapping Information Sharing Agreements and Data Privacy Impact Assessments.
- The Information Governance administrators will be responsible for the implementation and monitoring Information Governance Toolkit Standards and for the yearly returns to the Department of Health registering the Trust's compliance to the Standards.

2.7 **Information Security Officer**

2.7.1 The Associate Director of IT Strategy & Projects is the Trust's designated Information Security Officer.

They will work closely to ensure the implementation of information governance / cyber security practices across the organisation.

2.7.2 These Trust officers will also be responsible for the dissemination of staff awareness and training programmes in relation to information governance / security.

2.7.3 Attending the Information Governance Steering Sub-Committee on a regular basis and through the Committee maintaining the Trust's Information Security risk register.

2.8 **Data Protection Officer**

2.8.1 The Data Protection Officer is responsible for:

- Ensuring that appropriate Data Protection Act notifications are maintained for applicable Trust's systems and information.
- Dealing with enquiries, from any source, in relation to the GDPR, Data Protection Act and facilitating advice and support relating to formal subject access requests.
- Advising users of information systems, applications and networks on their responsibilities under the Data Protection Act, including subject access requests.
- Advising the Director of Information Technology on breaches of the Act and the recommended actions.
- Encouraging, monitoring and checking compliance with GDPR and the Data Protection Act.
- Liaising with external organisations on data protection matters.
- Promoting awareness and providing training, guidance and advice on GDPR and the Data Protection Act as it applies with the Trust.
- Ensuring all training is recorded and registered appropriately.

- To be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the organisation's privacy notice
- To have no conflict of interest.

2.9 **Information Asset Owners (IAO)**

2.9.1 Each information asset or new development will be assigned an Information Owner. Owners are responsible for:

- Ensuring that security is designed and built-in to new systems before initial deployment.
- Ensuring that adequate security is put in place for assets that existed before this policy was enacted.
- Ensuring that all assets and security processes associated with each individual system is identified, defined and documented.
- Ensuring that authorisation levels and procedures are clearly defined and documented.
- Ensuring that any delegated responsibility has been discharged correctly.

IAA - Provide support to the IAO's by:

- Ensuring that policies and procedures are followed
- Recognising potential or actual security incidents,
- Consulting the IAO on incident management,
- Ensuring that the information asset registers are accurate and maintained

2.10 **Freedom of Information Act (FOIA) Responsibilities**

2.10.1 The Legal Services Manager is the Trust Freedom of Information Officer and is responsible for:

- The central information access function, ensuring FOIA requirements are met.
- Providing professional advice and support on the release of information under the FOIA, researching and keeping up-to-date with legislation to ensure all advice is in line with legal requirements.
- Providing training and education awareness, undertaking presentations and workshops as appropriate to ensure all staff are aware of their responsibilities.

2.11 **Associate Director of Systems & I.G**

2.11.1 The **Associate Director of Systems & I.G** will be responsible for the implementation of the IT facility procedures detailed within this policy and its associated procedural guidelines.

2.11.2 The **Associate Director of Systems & I.G** will be responsible for ensuring information governance / security is considered when applications / systems are under development or enhancement.

2.12 Line Manager's Responsibilities

2.12.1 Line managers are directly responsible for:

- Ensuring the security of the Trust's assets, that is information, hardware and software used by staff and, where appropriate, by a third party, is consistent with legal and management requirements and obligations.
- Ensuring that this policy and its supporting procedures and guidelines are built into local processes and that their staff are aware of their security responsibilities and there is on-going compliance and adherence within their teams.
- Ensuring that their staff have had suitable mandatory information governance / security training.

2.13 General / All Staff Responsibilities

2.13.1 All staff, whether permanent, temporary, bank or contracted (including contractors), are responsible for ensuring that they are aware of the mandatory requirements place upon them, and for ensuring that they comply with the appropriate Trust procedures in relation to information governance / security and that it becomes an integral part of the day to day operations of the Trust.

2.13.2 All staff, or agents acting for or on behalf of the Trust, have a duty to:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the Trust's IT systems.
- Report on any actual or suspected breaches in information governance / security of this policy or its associated procedures; any weaknesses or potential threats to information governance / security. These breaches should be reported either on Datix and/or directly to their immediate line manager and the Information Governance Manager / Information Governance Officers as quickly as possible. Security incidents are not limited to "hacker activity" but include any incident that has / can cause harm to information assets, for example, operator errors and service outage.
- Act in an ethical and professional manner and ensure that all activities are conducted in a security conscious manner.
- Undertake mandatory information governance / security training on an annual basis.

Responsible Committees

2.14 Trust Board Responsibilities

2.14.1 There is Trust Board representation on the Information Governance Steering Sub-Committee to ensure that information governance is embedded within the Trust's structure.

.

2.15 **The Quality Committee Responsibilities**

2.15.1 Information Governance Management across the Trust will be co-ordinated by the Information Governance Steering Sub-Committee, which is accountable to the Trust Board.

2.16 **Information Governance Group Responsibilities**

2.16.1 The Trust's Information Governance Steering Sub-Committee has the responsibility for overseeing the implementation of the Information Governance Framework, the Information Governance Policy and the Information Governance Toolkit Assessment Plan.

2.17 **Trust Records Group Responsibilities**

2.17.1 The Trust's Records Group reports to the Information Governance Steering Sub-Committee to ensure information governance in relation to records management is embedded within the Trust's structure.

3.0 DEFINITIONS

3.1 **Information Governance**

- A framework which allows organisations and individuals to ensure that confidential information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care. It brings together all of the requirements, standards and best practice that apply to the handling of information.

3.2 **Data Security & Protection Toolkit (DSPT)**

- The web based application available via the NHS network which has been jointly developed by the Department of Health and the NHS Digital incorporating initiatives relating to matters such as confidentiality, data protection, freedom of information, information security, information quality assurance and health records management.

3.3 **Senior Information Risk Owner (SIRO)**

- An Executive member of staff that sits on the Board who will have overall responsibility for Information risk for the Trust.

3.4 **Personal Identifiable Information**

- Described in Article 4 - Definitions (GDPR) as factual information or expression of opinion which relates to an individual who can be identified from that information or in conjunction with any other information coming into possession of the data holder. Personal information includes; name, address, postcode, date of birth, staff details or any other unique identifier such as NHS Number, Hospital Number, National Insurance Number etc. It also includes information which, when presented in combination, may identify an individual e.g. Postcode, date of birth etc.

3.5 **Sensitive Information**

- Defined in Article 9 (GDPR) - special categories of personal data as data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings genetic, biometric or convictions. These sets of data are subject to more stringent conditions on their processing when compared to personal identifiable information.

3.6 **Confidential Information**

- Any information if leaked into the Public domain that could harm an individual or an Organisation.

4.0 PRINCIPLES

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

4.2 The Trust also recognises the need to share information with other health organisations and other agencies in a controlled manner, with the interests of the patient / staff, and in some circumstances, the public interest.

4.3 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 and managers to ensure and promote the quality of information and to actively use information in the decision making process.

4.4 There are four key connecting components to the information governance / security policy and its associated procedures:

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

4.4.1 **Openness**

- Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust code of openness.
- The Trust will establish and maintain policies and procedures to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.

- Patients will have ready access to information relation to their health care, their options for treatment and their rights as patients.
- Staff will have ready access to information in relation to their personnel records.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust will have clear procedures and arrangements for handling queries from patients, staff and the public.

4.4.2 **Legal Compliance**

- The Trust regards all identifiable personal information relation to patients and staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act, Human Rights Act and the common law on confidentiality.
- The Trust will establish and maintain policies and procedures for the controlled and appropriate sharing of patient / staff information with other agencies, taking account of relevant legislations (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

4.4.3 **Information Security**

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures, training and awareness.
- The Trust will establish and maintain incident reporting procedures, and will monitor and investigate all reported instances of actual potential breaches of confidentiality and security.

4.4.4 **Information Quality Assurance**

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records through its Records Management policy and procedures.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers will be expected to take ownership of, and seek to improve, the quality of information within their services.
- Data standards will be set through clear and consistent definitions of data items, in accordance with national standards.

- The Trust will promote information quality and effective records management through policies, procedures / users manuals and training.

It also aims to support the requirements of:

- **Accountability:** accounting for the actions of individuals by monitoring their activities.

- **Non-Repudiation:** legally acceptable assurance that transmitted information has been issued from and received by the correct, appropriately authorised, individuals

All parts of the organisation are responsible for making sure that information is protected adequately. Senior management recognise the sensitive nature of the information that the organisation stores and processes, and the serious potential harm that could be caused by security incidents affecting this information. They will therefore give the highest priority to information security. This will mean that security matters will be considered as a high priority in making any business decisions. This will help the Trust to allocate sufficient human, technical and financial resources to information security management, and to take appropriate action in response to all violations of Security Policy.

5.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE

5.1 It is the policy of the Trust to ensure that all staffs, and partner organisations, comply with any statutory obligations relating to information governance / security.

5.2 **Identification of Relevant Legislation**

5.2.1 The Trust will ensure that for each of its information systems it has identified all relevant statutory, regulatory and contractual requirements pertaining to the systems, and that individual responsibilities to meet these requirements are defined within the appropriate job descriptions.

5.3 Any use of personal identifiable information must comply with the legislation listed below; enquiries should be addressed to the Data Protection Officer or Information Governance Manager:

- General Data Protection Regulation
- The Data Protection Act (2018
- The Freedom of Information Act (2000)
- The Human Rights Act (2000)
- The Common Law Duty of Confidentiality
- The Copyright, Designs and Patents Act (1990)
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- Health and Social Care Act (2000) (*this list is not exhaustive*)

5.4 **Control of Proprietary Software Copying**

5.4.1 The Copyright Designs and Patents Act 1988 controls the copying of software. No copyright material will be copied without the copyright owner's consent. All enquiries are to be addressed to the Head of IT.

5.5 **Safeguarding of Trust Records**

5.5.1 The Trust will ensure that important records are protected from loss or destruction. This will include, but will not necessary be limited to, records that must be retained to meet statutory requirements and those records required to support the Trust's essential business activities.

5.5.2 Guidance for the appropriate storage, retention and destruction of records within the Trust is provided in the Storage, Retention and Destruction of Records Procedure. Any enquires should be addressed to the Records Manager.

5.6 **Data Protection and Privacy of Personal Information**

5.6.1 The Trust's Data Protection Officer is also the Legal Services Manager, who will ensure that appropriate controls are in place to protect the privacy of personal information in accordance with the requirements of the General Data Protection Regulation and the Data Protection Act 2018.

5.7 All employees of the Trust must be aware of the requirements of the legislation. It is the responsibility of all senior managers (Information Asset Owners) within the Trust to ensure that any current or proposed use of personal information within their area of responsibility complies with the Trust's Data Protection registered purposes.

5.8 **Caldicott Recommendations**

5.8.1 The Trust will comply with the recommendations of the Caldicott Report into the use of patient identifiable information within the NHS. All uses of patient identifiable information within the Trust must comply with the Caldicott principles of good practice. Any enquiries should be addressed to the Caldicott Guardian.

5.9 **Information Sharing**

5.9.1 The sharing of confidential patient-identifiable information should be governed by clear and transparent procedures that satisfy the requirements of law and guidance and regulate working practices in both the disclosing and receiving organisations. In some circumstances these procedures and the underpinning standards should set out within an agreed information sharing agreement or protocol. A Data Privacy Impact Assessment is also required to assess risk to any data transfers or change of use/ implementation of a new system or change to a system. Both will identify the legal basis for sharing data appropriate to the purpose.

5.9.2 The Trust will need to share confidential patient-identifiable information with a range of organisations. The purpose to be served by sharing information will either relate to the provision of care, including the quality assurance of that care, for the individual concerned or will be for non-care or secondary purposes e.g. service evaluation, patient complaints or care enquiries, research, finance, public health work etc.

5.9.3 Information sharing agreements can be a useful way of providing a transparent and level playing field for organisations that need to exchange information. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing patients about the possibility of sharing and the choices they have to limit sharing. If the patients say no to sharing, then information may only be shared in exceptional circumstances. The lawful basis for sharing must be ascertained in all circumstances.

5.9.4 Information partners can be, but not limited to:

- NHS Organisations
- Social Care and other Local Authority elements
- The Police
- Sure Start Teams
- Education Services
- Voluntary Sector Providers
- Private Sector Providers

5.9.5 All information sharing agreements will be regularly reviewed and updated. The identification, documentation and protocols for sharing patient-identifiable information will be agreed with all new information sharing partners.

5.9.6 Please refer to the Trust's Information Sharing & Consent Policy/Procedure for additional guidance on information sharing.

5.10 Prevention of Misuse of IT&T Facilities

5.10.1 All employees of the Trust (those working for or on behalf of the Trust) and any third party users will not be granted access rights to any Trust system unless formal authorisation has been given by the IT&T Department.

5.10.2 Failure to comply with this could be in breach of the Computer Misuse Act 1990, which may lead to disciplinary action in accordance with Trust Policy.

5.11 **Year on Year Improvement Plan and Assessment**

5.11.1 An assessment of compliance with requirements, within the Information Governance Toolkit will be undertaken each year. The results of the return will be monitored along with any action / development plan by the Information Governance Steering Sub-Committee. The Executive Chief Finance Officer (SIRO) will report on the progress of the Trust against the Toolkit to the Quality Committee. The annual assessment will be submitted to the Quality Committee for ratification. The requirements are grouped into the following initiatives;

- Information Governance Management
- Confidentiality and Data Protection
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information assurance

5.11.2 Trusts are required to complete annual self-assessments against the Information Governance Toolkit requirements by 31st March each year.

6.0 SCOPE OF POLICY

6.1 This document applies Trustwide to all services and employees of EPUT without exception.

6.2 This policy and its associated procedural guidelines applies to and must be read and observed by all staff, including contracted, non-contracted, temporary, honorary, secondments, bank, agency, students, volunteers or locums, wishing to use the Trust's information / data facilities and / or systems, prior to their doing so.

6.3 This policy and its associated procedures cover all information / data systems purchased, developed and managed by, or on behalf of EPUT and all individuals directly employed or otherwise by the trust.

6.4 For the purpose of this policy and its associated procedures information / data is defined as information / data that is stored in any media, for example:

- Paper
- Electronic
- Audio or visual
- Passed on verbally

6.5 This policy and its associated procedures cover all aspects of information / data, including:

- Patient / client / service user
- Personnel / staff
- Organisational / corporate

6.6 This policy and its associated procedures cover all aspects of information / data, including:

- Structured record systems (paper and electronic)
- Unstructured information (paper and electronic)
- Transmission of information (fax, e-mail, post, telephone, internet)

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

7.0 MONITORING, REVIEW AND PERFORMANCE MANAGEMENT

7.1 The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust.

7.2 The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate.

7.3 The Executive Chief Finance Officer (SIRO) & Clinical Support is the specific senior manager responsible for co-ordinating, publicising and monitoring implementation of this policy and its associated procedural guidelines.

7.4 This policy and its associated procedural guidelines will be reviewed every three years in line with Trust policy or whenever legislation, national or local guidance requires.

7.5 The Information Governance Manager, Information Security Officers and Information Asset Owners (as defined within the Trust's Information Asset Register held by the Information Governance Leads) will be responsible for ensuring the implementation of this policy and its associated procedures, as appropriate.

7.6 The Information Governance Manager and / or Information Security Officer will provide the Information Governance Steering Sub Committee, Quality Committee and Executive Team with relevant reports on information governance / security developments, breaches, changes in legislation / guidance and facility usage on a regular basis (minimum quarterly).

7.7 The Trust will work towards full and continued compliance to information security management systems, ensuring independent audits are undertaken, as appropriate or dictated by guidance:

- Information Governance Toolkit (IG Toolkit) standards
- Care Quality Commission (CQC)
- Internal Auditors
- NHS Litigation Authority (NHSLA)

8.0 ABUSE OF TRUST FACILITIES

8.1 Any employee found to be in breach of information governance / security guidance may be investigated pending disciplinary procedures in line with Trust policy and may be subject to formal proceedings.

8.2 In the event of abuse of any Trust information / data systems / services all access will be immediately revoked pending any investigation. This will include:

- the deliberate accessing, viewing, downloading or distributing of:
    - Information not related to role (e.g. accessing their own / friends / family information).
    - Pornographic or otherwise offensive material.
- the use of portable media (i.e. laptops, USB Keys, mobile phones, PDA etc.) to store / transfer person identifiable data.
- not adhering to clear desk policy (safe, secure storage of manual records in empty offices).

8.3 Such acts would be regarded as gross misconduct under the Trust's disciplinary procedures and the use / transfer of person identifiable or sensitive data / information outside of Trust procedures. Any employee found to have been engaging in such activities will be investigated through the disciplinary procedures in line with Trust policy and may be subject to formal proceedings.

9.0 TRAINING

9.1 The Trust will maintain a high level of information governance / security awareness within the organisation by ensuring that all staff receive appropriate, job relevant, training. This may include:

- Team Briefings
- Publications via Electronic Staff Briefings
- On-Line training via the NHS DIGITAL Information Governance website.
- OLM Training
- It will be a mandatory requirement for all staff involved in any type of information governance / security breach to complete training, irrespective of previous sessions.
- Training will be done in accordance with the Induction and Mandatory Training Policy.

10.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES

Information Governance/Security Procedural Guidelines

CPG50 – Information Governance & Security Procedure
CPG50A – ITT Security Procedure
CPG50B – Email, Intranet, Internet Access & Use Procedure
CPG50C – Safe Haven Procedure
CPG50D – Information Governance Incident Reporting Procedure
CPG50E – Data Privacy Impact Assessment Procedure
CPG50F – SMS Text Messaging to Service Users Procedure
CPG50G – Information Asset Register Procedure
CPG50H – NHSMail Usage Procedure
CPG50I – Not used

END