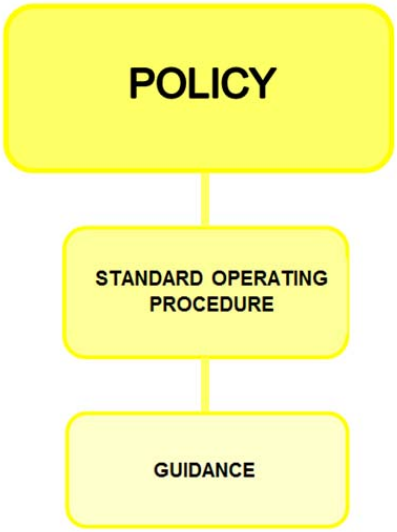
Lancashire Care NHS
NHS Foundation Trust

INFORMATION MANAGEMENT & TECHNOLOGY SECURITY POLICY

(Includes Access, Acceptable Use, Electronic Communications and Mobile Devices Security)

UNIQUE POLICY REFERENCE	IMT 003
APPROVAL DATE	27 February 2017
REVIEW DATE	27 February 2018
POLICY AUTHOR	Information Governance, Assurance & Compliance Lead
ACCOUNTABLE DIRECTOR	Executive Director of Finance, HI & Estates (SIRO)
APPROVED BY	Deputy SIRO

TRUST GOVERNANCE STRUCTURE
POLICY LINKED TO Infrastructure Sub Committee



POLICY VERSION CONTROL

This record shall detail all previous versions of the Policy, including versions that have been known by other names and the date of when a new version was created.

Previous Versions (Title)	Date Reviewed	Why was a new version created?
Information Management and Technology Security Policy V2	*Dec 2016*	*Policy written in new corporate format and incorporates Electronic Communications Policy and details of IAO structure – main content is in the supporting Standard Operating Procedure*
No change	*Nov 2017*	*Change to reflect ISO 27000:1 commitment*

1. TRUST POLICY STATEMENT

The purpose of this policy is to protect the information assets of Lancashire Care NHS Foundation Trust and comply with all relevant legislation.

The Trust has a legal obligation to protect the lifecycle of all its data. All electronic and paper based information whether it is patient or business related must be treated securely and confidentially and are subject to record keeping, archiving, and legal processes. The Trust is working towards ISO27001 Certification to meet this requirement.

Legislation directly relating to this policy is:

- Data Protection Act, 1998
- Access to Health Records Act 1990
- Freedom of Information Act, 2000
- The Human Rights Act 1998
- Computer Misuse Act, 1990
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act, 1993
- Health & Social Care Act 2001
- Caldicott Guidelines
- Common Law duty of Confidentiality
- Privacy of Electronics Communications Regulation (PECR) 2016
- The Employment Practices Data Protection Code Part 3:Monitoring at Work
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Obscene Publications Act 1964
- Protection of Children Act 1978
- Defamation Act 1996
- Criminal Justice and Public Order Act 1994

2. APPLICATION

This policy applies to information (data), which is created, processed, stored, transmitted or received and is held in filing systems, on any form of computer, including laptops, mobile phones, smartphone devices, tablets and USB devices.

The intent of this policy and associated procedures is to set out clear guidance on safe and secure access, use and appropriate conduct of electronic communication facilities, to enable effective communication and simultaneously support the business functions of the Trust.

This Policy applies to all Trust employees, other persons working for or on behalf of the Trust and usage by anyone granted access to the Trust network or systems. It is applicable to all business functions and information contained on the network, the physical environment and relevant people who support the network.

3. IMPLEMENTATION

All users of the Trust's electronic communication facilities are obliged to adhere to this Policy. It is the responsibility of each individual to ensure that they understand the Policy and any other associated Trust Policies, Procedures and Guidelines referred to in this Policy. A failure to adhere to the Policy may result in disciplinary action.

Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of, and adhere to, the Policy. They are also responsible for ensuring that their staff have the appropriate skills and training and are updated in regard to any changes to the Policy.

In order to comply with the Policy staff must refer to the following procedures and guidance documents:

- Information Management & Technology Security Procedure
- Procedure for Communicating via E-mail, Text Messaging (SMS) and Video Communication

Staff should also be aware that other policies may have implications with regard to the adherence to this policy and therefore they should, were appropriate, familiarise themselves with the following policies, procedures and guidance:

- Corporate Records Management Policy and Procedure
- Mobile Communication Devices Policy
- Health Records Service Security and Confidentiality Policy
- Access to Health Records Policy
- Professional Record Keeping Policy
- Data Quality Policy
- Health Records Management Policy
- Policy for Sharing & Disclosure of Service User Related Information with External Agencies
- RA Policy and Procedure
- Information Governance Toolkit -
- IT Infrastructure Library (ITIL) Standards
- Information Commissioners Office (ICO) Guidance for Information Security Management
- Department of Health Guidance for Information Security Management

Please refer to IT Clinical Systems Training site for clinical systems guidance documents.

Local Standard Operating Procedures and Protocols are permitted but they must be compliant with Trust policy and must not contradict or dilute any guidance.

4. COMPLIANCE

All employees are responsible for ensuring that breaches of information security do not result from their actions and that they have made themselves familiar with their security responsibilities before handling data or using data processing systems.

Line Managers must ensure that all employees are updated and informed of their security responsibilities. An adequate confidentiality clause should be contained in contracts of employment and periodically reviewed.

Line Managers are responsible for ensuring that their staff and contractors understand their roles and responsibilities. Line management are also responsible for ensuring the security of the Trust information assets (that is information, hardware and software used by staff and where appropriate by third parties) is consistent with legal and management requirements and obligations.

All staff or agents acting for the Trust have a duty to safeguard hardware, software and information in their care including the reporting of incidents and near misses e.g. confidential information being incorrectly or insecurely stored, sent to an incorrect destination or recipient, theft or loss of equipment. For a full list of line manager and user responsibilities please refer to the Information Management and Technology Security Procedure.

Every person in the organisation has a responsibility for data protection. The Trust processes sensitive personal data and everyone has an obligation to protect this data. All employees must make themselves familiar with Data Protection Guidance. Refer to the Data Protection Principles and the Trust Information Security Guidelines.

5. COMMUNICATION

A range of communication methods will be used to raise awareness of the new Policy. This will include via the Trust News bulletin, Trust wide email, uploading the policy to the My Compliance portal and the delivery of the Policy to each user's desktop if required. The Policy will be accompanied by a short User Survey to gauge understanding of the Policy. Each user will also be asked to confirm receipt of the Policy and confirm that they have read and understood it.

For further information please refer to the communication plan for this policy.

6. MONITORING INTEGRITY OF THE SYSTEM

Use of the Trust's data processing systems is subject to monitoring by the Health Informatics department. All employees should be aware that email and Internet usage is monitored (Regulation of Investigatory Powers Act 2000) to ensure compliance with legislation i.e. the Data Protection Act 1998 and the Computer Misuse Act 1990 and Trust Policy.

Standard	**Time frame/ format**	**How**	**Whom**
IG Toolkit Requirements	Annually	Self-Assessment	IG Team
Information Governance e-learning	Annually	Completion of an online e-learning training module hosted by NHS Digital or other nominated provider.	Individual responsibility
NHS Security Standards	As per Internal	Audit	Internal

	audit schedule		Auditors
	As per external audit schedule	Audit	External Auditors
NHS Security Standards and DPA	Annually	User Access Audits	HI Team
Data Protection Act 1998	Ad hoc	Investigation of IT systems	IT Service
Computer Misuse Act 1990	Ad Hoc	Investigation of IT systems	IT Service

This policy will be implemented in line with NHSLA requirements, Monitor Authorisation and the Information Governance Toolkit requirements to ensure the effectiveness of its implementation and staff knowledge and understanding of the content