Directorate of Strategy & Planning

INFORMATION SECURITY POLICY

Reference:	DCP080
Version:	1.7
This version issued:	01/03/17
Result of last review:	Minor changes
Date approved by owner (if applicable):	N/A
Date approved:	28/02/17
Approving body:	Information Governance Steering Group
Date for review:	February, 2020
Owner:	Pam Clipson, Director of Strategy & Planning
Document type:	Policy
Number of pages:	8 (including front sheet)
Author / Contact:	Linda Da Costa, Information Services Manager

1.0 Background

1.1 At Northern Lincolnshire & Goole NHS Foundation Trust where information processing is a fundamental part of its purpose. It is important, therefore, that the organisation has a clear and relevant Information Security Policy, allowing it to comply with information legislation.

1.2 The purpose of Trust's Information Security policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially; it encompasses the behaviour of the people who manage information in the line of with the Trust's business.

1.3 Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way
- Assurance that the Trust is providing a secure and trusted environment for the management of information used in delivering its business
- Clarity over the personal responsibilities around information security expected of staff when working with the Trust's information
- A strengthened position in the event of any legal action that may be taken against the Trust
- Demonstration of best practice in information security
- Assurance that information is accessible only to those authorised to have access
- Assurance that risks are identified and appropriate controls are implemented and documented

2.0 Aim

The aim of the Trust's Information Security Policy is to preserve:

Confidentiality	Access to Data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

3.0 Objectives

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

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies
- Describing the principles of security and explaining how they shall be implemented in the Trust. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities
- Creating and maintaining within the Trust a level of awareness of the need for Information Security as an integral part of the day to day business
- Protecting information assets under the control of the organisation

4.0 Area

The scope of this Policy is the Information Security of the Northern Lincolnshire and Goole NHS Foundation Trust.

5.0 Duties, Roles and Responsibilities

5.1 Chief Executive

Information Security is everyone's business although responsibility resides ultimately with the Chief Executive but this responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO) and Information Security Officer as required by the Information Governance Toolkit.

5.2 Senior Information Risk Owner (SIRO)

5.2.1 The Senior Information Risk Owner (SIRO) is responsible for information risk within the Trust and advises the Board on the effectiveness of information risk management across the Organisation.

5.2.2 The SIRO has responsibility for ensuring key contractors or support organisations (including non-clinical staff) that have access to information and/or other information assets have been reviewed to ensue written contract adequately cover compliance with information governance requirements.

5.3 Senior Managers

Senior Managers shall be individually responsible for the security of their area where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor
- Are aware of the information security policies, procedures and user obligations applicable to their area of work
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using
- Ensuring staff know how to access advice on information security matters

5.4 Information Security Officer (Associate Director of IM&T)

5.4.1 The Information Security Officer will:

- Hold a relevant qualification in Information Security
- Have lead responsibility for information security management within the Trust
- Acting as a central point of contact on information security for both staff and external organisations
- Manage and implement this policy and related procedures
- Monitor potential and actual security breaches
- Ensure that staff are aware of their responsibilities and accountability for information security
- Ensure compliance with relevant legislation and regulations

5.4.2 In carrying out these tasks the Information Security Officer will work closely with the IT Manager/Systems Development Manager and the Trust Information Governance Lead.

5.5 All Staff

5.5.1 All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should understand:

- What information they are using, how it should be protectively handled, stored and transferred
- What procedures, standards and protocols exist for the sharing of information with others

- How to report a suspected beach of information security within the organisation
- Their responsibility for raising any information security concerns with the Information Security Officer (Associate Director of IM&T)

5.5.2 Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

6.0 Policy Framework

6.1 Contracts of Employment

6.1.1 Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

6.1.2 Information security expectations of staff shall be included within appropriate job definitions.

6.2 Security Control of Assets

6.2.1 The Trust has an Information Asset Management Register listing all associated system; this includes the Information Asset Owners and Asset Administrators.

6.2.2 All the Trust's assets shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

6.3 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO.

6.4 Computer Access Controls

Access to IT facilities shall be restricted to authorised users who have business need to use the facilities.

6.5 Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.6 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be; identified, registered and physically protected from threats and environmental hazards.

6.7 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of the Trust.

6.8 Information Risk Assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risks assessments are performed at least annually, following guidance form the Senior Information Risk Owner (SIRO).

6.9 Information Security Events and Weaknesses

All the Trust's information security events and suspected weaknesses are to be reported to the Information Security Officer or designated deputy and where appropriate reported as an Adverse Incident.

6.10 Classification of Sensitive Information

The Trust shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their information assets.

6.11 Monitoring System Access and Use

6.11.1 An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The Trust will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training) in the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system

6.11.2 Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

6.12 Accreditation of Information Systems

The Trust shall ensure that the key information systems, applications and networks include a System Level Security Policy (SLSP).

6.13 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the IT Manager and Systems Development Manager.

6.14 Business Continuity and Disaster Recovery Plans

6.14.1 The organisation will implement a business continuity management system (BCMS) in line with best practice.

6.14.2 Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

6.14.3 The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

6.15 Training & Awareness

Information Governance training is mandatory and all staff are required to complete annual Information Governance training.

7.0 Monitoring Compliance and Effectiveness

7.1 Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Steering Group, together with independent reviews by both Internal and External Audit on a periodic basis.

7.2 The Information Services Manager is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises depending on National Guidance.

8.0 Associated Documents

None.

9.0 References

None.

10.0 Definitions

10.1 **BCMS** – Business Continuity Management System.

10.2 **IAO** – Information Asset Owner.

10.3 **SIRO** – Senior Information Risk Owner.

10.4 **SLSP** – System Level Security Policy.

11.0 Consultation

Information Governance Steering Group.

12.0 Equality Act (2010)

12.1 In accordance with the Equality Act (2010), the Trust will make reasonable adjustments to the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. The Trust will endeavour to develop an environment within which individuals feel able to disclose any disability or condition which may have a long term and substantial effect on their ability to carry out their normal day to day activities.

12.2 The Trust will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Trust's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010).

The electronic master copy of this document is held by Document Control, Directorate of Performance Assurance, NL&G NHS Foundation Trust.