WE'RE PROUD TO CARE

Chesterfield Royal Hospital NHS
NHS Foundation Trust

INFORMATION SECURITY POLICY

1. INTRODUCTION

1.1 Data stored in the Trust’s information systems represents a valuable asset. The reliance of the Trust on information to deliver value to its Staff and Service Users, by meeting agreed service levels and corporate objectives makes it necessary to ensure that the systems developed, used and maintained facilitate the provision of a safe, secure and reliable infrastructure.

2. POLICY STATEMENT

2.1 The Trust recognises the need for, and is committed to achieving, exceptional levels of security to maintain the confidentiality, integrity and availability of all electronic information. This policy defines how the trust will work towards this goal, as required by the HSCIC.

3. DEFINITIONS

3.1 Staff
All permanent, temporary and contracted employees fall within scope of this document.

3.2 Sites
This Policy applies to **Chesterfield Royal Hospital Foundation Trust** and all other sites from which the Trust delivers or manages Services.

4. ROLES AND RESPONSIBILITIES

4.1 The Trust and its Board of Directors have agreed the appointment of the following individuals to carry out the tasks as required by the HSCIC.

4.2 Chief Executive
The Trust’s Chief Executive is the Accounting Officer and has overall accountability for:

- Information Security
- Assessment and mitigation of Information Security risks

4.3 Senior Information Risk Owner (SIRO)
The Trust’s SIRO is responsible for the management of Information Risks within the Trust.

4.4 Head of Information and Communications Technology
The Head of ICT has overall responsibility for the security of the entire IT infrastructure. This is comprised of the Live, Project (under development) and Test Environments managed and maintained by the ICT Department.

4.5 ICT Operations Manager
The ICT Operations Manager has overall responsibility for the security of all Live IT

Services.

4.6 IT Programme Manager
The IT Programme Manager has overall responsibility for the security of all IT Services in Project phase (under development).

4.7 Technical Service Manager (TSM)
The Technical Service Managers are responsible for the day-to-day running of all their IT Technical Services. It is the TSMs' responsibility to manage the security aspects of their Technical Services.

4.8 Information Security Officer (ISO)
The Trust's ISO is the Head of ICT who will:

- 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

4.9 Senior Managers
Senior Managers shall be individually responsible for the security of their physical environments 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.

4.10 Staff
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 organization.
- Their responsibility for raising any information security concerns with the Information Security Officer.

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.

5. IT SECURITY POLICY FRAMEWORK

5.1 Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.2 Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.3 Access Control
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.

5.4 Computer Access Controls
Access to ICT facilities shall be restricted to authorised users who have business need to use the facilities.

5.5 Application Access Controls

5.6 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 both the availability of a licence and approval from your Line Manager to purchase license(s).

5.7 Authorised users, as noted above, may not access and/or alter their own medical or corporate records.

5.8 Authorised users, as noted above, may not access and/or alter a relative’s medical or corporate record.

5.9 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.

5.10 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.

5.11 Information Risk Assessment
All information assets will be identified and assigned an Information Asset Owner (IAO). IAOs shall ensure that information risks assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). This should be

increased to quarterly for all 'major' assets. IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Please see the Information Risk Procedures for further information.

5.12 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported to the Information Security Officer or designated deputy and reported on **Datix** as an Information Security Incident. Please see the incident reporting policy for further information.

5.13 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. Further details of the classifications controls can be found in the Risk Management Policy.

5.14 Protection from Malicious Software

The organisation and its Corporate ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Head of ICT. Users breaching this requirement may be subject to disciplinary action.

5.15 Data Back-up and Housekeeping

It is the responsibility of the IAO to ensure a backup policy is in place, for all their information assets, and that it is executed as agreed.

5.16 Removable Media

All removable media must be preconfigured with encryption software prior to use. Removable media that contain software require the approval of the Head of ICT before they may be used on Trust systems. Users breaching this requirement may be subject to disciplinary action. Staff may refer to the Policy for the Use and Secure Disposal of Removable Media.

5.17 Monitoring System Access and Use

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.

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

5.18 Accreditation of Information Systems
The organisation shall ensure that all new information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the Information Security Officer and/or ICT Operations Manager before they commence operation.

5.19 Change Advisory Board
Changes to information systems, applications or networks shall be reviewed and approved by the Change Advisory Board and the Information Security Officer.

5.20 Existing Systems Failing to Meet Security Standards

5.21 Where existing systems fail to meet standards outlined in the policy, and can be made to comply, it will be the responsibility of the relevant IAO to ensure that the issue is rectified within an agreed timescale.

5.22 Where a system is incapable of complying, the IM&T Steering Group has the option of:

- Granting an exemption
- Amending the system
- Requiring a replacement system to be commissioned

5.23 Business Continuity and Disaster Recovery Plans:

5.24 The Trust has an IM&T Disaster Contingency Policy to react and/or minimise the impact of any major unforeseen failure that could impair Trust processes.

5.25 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.

5.26 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.

6.0 TRAINING

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

7.0 DISSEMINATION

7.1 Intranet
This policy is available to all staff on the Trust's Intranet.

7.2 Notice
As a minimum, all staff will be notified of this policy through one of the following means:

- Local Induction

- Email from Briefing Staff, Communications Team
- Line Manager
- Team Meeting

8.0 MONITORING

8.1 The ISO is responsible for the monitoring, revision and updating of this document on an annual basis or when required.

9.0 COMPLIANCE

9.1 Any deviation from this policy or related policies should be reported to the Service Desk as a Security Incident. IT will follow the Datix Procedure for reporting IT Security Incidents and act accordingly. In certain circumstances, HR advice and support may be sought and appropriate action may be taken in line with the Trust's Disciplinary Policy. Where there are reasonable grounds for believing that a crime may have been committed the Trust's Security Advisor will be notified and the Police will be informed forthwith.

10. KEYWORDS

10.1 Information Security Policy

10. RELATED POLICIES

10.1

- Acceptable Use Policy
- IM&T Disaster Contingency Policy
- Computer Software-Based Threats Policy
- Safe Haven Policy
- Disposal of IT Equipment and Assets Policy
- Computer Equipment Taken Off Site Policy
- E-Mail Policy
- Internet Policy
- PDA Policy
- Remote Access to Email Policy
- Policy of the use and secure disposal of removable storage media

11. REFERENCES

11.1

- NHS England Information Security Policy
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order (2000).
- The Copyright, Designs and Patents Act (1988)

- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)

Health & Social Care Act (2012)

12.0 GLOSSARY

12.1 **Availability**

- Describes the accessibility and usefulness of Information to authorised users at times when they require it

Confidentiality

- It is the security of Information against unauthorised access.

Integrity

- It is the property of preserving the accuracy and completeness of information.

Live IT Services

- IT Services which have been signed off by the ICT Operations Manager and turned over to production.

13.0 EQUALITY IMPACT ASSESSMENT

13.1 Please see Appendix A

Date ratified:	Hospital Leadership Team – July 2016
First issued:	April 2000
Version no:	2.0
Date issued:	July 2016
Review date:	July 2018
For review by:	ICT Quality and Governance Manager
Director responsible:	Director of Nursing and Patient Care

EQUALITY IMPACT ASSESSMENT Appendix A

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability – learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**here any evidence that some groups are affected differently?**	No	
3.	**you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?**	None identified	
4.	**he impact of the policy/guidance likely to be negative?**	No	
5.	**o can the impact be avoided?**	N/A	
6.	**at alternative are there to achieving the policy/guidance without impact?**	N/A	
7.	**n we reduce the impact by taking different action?**	N/A	