INFORMATION SECURITY POLICY

Version:	V6.0
Policy Author:	Naomi Wills
Designation:	Head of Information Governance
Responsible Director:	Director of Nursing and Quality
EIA Assessed:	04/02/2016
Target Audience:	All Trust Staff
Approved By:	Policy Review Group
Date Approved:	25/01/2016
Ratified By:	Policy Review Group
Date Ratified:	25/01/2016
Next Review Date:	25/01/2017

CONTENTS

1. Introduction

Information is one of the Trust's most important assets. The Trust and its staff have responsibilities and legal requirements to keep information safe, secure and confidential at all times. Particular care must be taken with both patient and staff personal confidential data.

The Trust will comply with all relevant legislation, this includes:-

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs & Patents Act 1988
- The Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000
- Data Retention and Investigatory Powers Act 2014

The Trust is also required to comply with the NHS Information Governance Assurance Statement and the requirements in order to link to the national N3 network.

This policy provides a high level overview of the Trust's commitment to ensure effective information security management. The following policies must be read in conjunction with this: -

- Email Usage Policy
- Internet Usage Policy
- Laptop Usage Policy
- Removable Media/Devices Policy

The Trust's Safe Haven Policy must also be adhered to.

2. Purpose

This policy aims to establish and maintain the security and confidentiality of information, information systems, applications, and networks owned or held by the Trust.

3. Definitions

3.1 N3 Network / Trust Network

The national secure NHS network to which Trust Computers / Laptops are connection

3.2 Server

The server runs the administrative software that controls access the network and its resources.

3.3 Firewall

Is a device that blocks unauthorised access to an organisation's local area network (LAN).

The firewall sits on the server acts as the LAN's gateway to the internet, or it can be a dedicated computer placed between the LAN and the Internet, so that the network is never in direct contact with the Internet.

The firewall also keeps track of every file entering or leaving the local area network in order to detect the sources of viruses and other problems that might enter the network.

3.4 Asset(s)

Any information system, computer or programme owned by the Trust and which stores data.

3.5 Encryption

Encryption is a way to enhance the security of a file by scrambling the contents so that it can be read only by someone who has the right password to unscramble it. Encryption software turns text into code format, therefore undecipherable.

Encryption software must be provided by the Information Technology Department. Your own software is not accepted by the Trust and may not meet the Department of Health's specifications.

3.6 Software

Computer programmes sometimes also called applications.

3.7 Virus

An unauthorised piece of computer code attached to a computer programme which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.

3.8 Cyber Security

Cyber Security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

4. Duties/Responsibilities

4.1 Chief Executive

The Chief Executive has ultimate accountability for information security within the Trust, ensuring systems and processes are in place to adequately meet its requirements.

4.2 Director of Nursing and Quality

The Director of Nursing and Quality is responsible for ensuring processes are in place for the safeguarding of information during storage and transfer.

4.3 Interim Director of Strategy and Business Support

The Interim Director of Strategy and Business Support is responsible for ensuring systems and equipment are in place to allow for the safeguarding of information on the Trust's Server and virus protection and encryption software is available.

4.4 Senior Information Risk Owner (SIRO)

The SIRO is the designated Board member responsible for the reporting of information security risks. The SIRO will report to the Trust Board.

4.5 Caldicott Guardian

The Trust's Caldicott Guardian is responsible for ensuring that the Trust is compliant with the confidentiality requirements of the Data Protection Act 1998.

4.6 Information Governance Group

The Information Governance Group is responsible for the implementation of the Information Governance work programme.

Compliance reports will be received and reviewed and where non compliance is identified action will be agreed and monitored by the committee.

4.7 Head of Information Governance

The Head of Information Governance is responsible for ensuring procedures are implemented to ensure the safeguarding of information.

They will advice the Information Governance Group on non-compliance and provide advice and support to staff as required.

4.8 Head of Information Security

The Information Technology Department is responsible for the day

to day operational management of all technical security processes. This is overseen and reviewed by the Head of Information Security who is a member of the Information Governance Group and who is responsible for reporting to the Information Governance Group in regard to IT risks.

The IT Department are responsible for the implementation and management of technical controls which are designed to protect information held within the Trust's IT environments.

IT Department is responsible for managing and maintaining the Asset Register and assigning Asset Owners for All Trust IT equipment.

4.9 Information Asset Owners/Information Asset Administrators

Information Asset Owners/Information Asset Administrators are responsible for ensuring that information assets are secured against the threats to them to an appropriate degree.

4.10 Staff

All staff are responsible for ensuring they comply with this policy and all other associated policies and procedures.

Security of requirements will be addressed at the recruitment stage and of contracts of employment will contain a confidentiality clause.

Security requirements will be included in job definitions where required.

All staff have a duty to report any actual or potential information security incidents.

5. Process

5.1 Asset Register / Asset Owners

The Trust must have an up to date Asset Register.

The Asset Register will be maintained by the Information Technology Department and reviewed annually. This will include: -

- Information assets: databases, data files, archived information
- Software assets: system software, application software
- Physical assets: computer equipment, technical equipment

Every asset (hardware, software, application or data system) will have a named Asset Owner who will be responsible for the security of that asset.

5.2 Access Controls

Only authorised personnel who have a justified and an approved business need can be given access to restricted areas i.e. information systems or stored data.

Access controls will be managed in adherence with the Trust's System Level Security Policy.

5.3 Remote Access

Remote access can be made available to staff as appropriate, with manager approval. Remote Access must be made via the Information Technology Department procedures.

5.4 Internet Connections

Where Trust equipment is connected to a network, connection to the internet is only permitted through the connection provided by the Information Technology Department

The Internet must be used in adherence with the Trust's Internet Usage Policy.

5.5 Password Management

Staff will have passwords in order to access restricted areas i.e. information systems or stored data.

Staff must ensure passwords remain secure at all times and must not be shared with others.

All actions taken during your log in will be monitored by the Information Technology Department and any inappropriate or misuse may result in disciplinary action.

5.6 Email Access

Staff must only use email accounts approved for use and assigned by the Information Technology Department.

Personal email accounts must not be used for business purposes.

Email must be used in adherence with the Trust's Email Usage Policy.

5.7 Removable Media / Devices

Staff must only use removable media / devices approved for use by the Information Technology Department with the exception of personal USB memory sticks. These will be managed by forcing encryption if plugged into Trust computers linked to the Network.

Removable media / devices must be used in adherence with the Trust's Removable Media/Devices Policy.

5.8 Storing / Saving Information

When saving information this must be done using Trust computers / laptops connected to the server only or other agile devices that are linked to the Trust's Network or have the ability to be uploaded to the Trust Network. Information must not be stored to r home drives or personal equipment. The Trust supported equipment is secure and also enables regular back-ups to be taken by the Information Technology Department to ensure loss of data is kept to a minimum during service disruption. .

Information must never be stored on the desktop or C: drive – these areas are not backed-up to the Trust server and can be accessed by anyone using that machine.

5.9 Physical & Environmental Security

To maintain availability of services, critical IT equipment such as servers and core networking equipment will be protected against physical and environmental threats such as:

- theft, vandalism, and accidental damage
- fire & flood damage
- overheating
- loss of power

The Information Technology Department will assess the risks to critical IT equipment and will provide the necessary facilities and resources to adequately mitigate the risks.

All PC's and servers under the control of the Trust will be protected from electronic threats such as viruses.

5.10 Firewalls

The Information Technology Department will be required to configure the network to include firewalls to ensure, as afar as is practical, separation of the Trust's networks from other networks.

The Information Technology Department will be required to position firewalls to protect any particularly sensitive servers or other equipment from other parts of the network. For example, if it is not possible to load anti virus software on a particular server, the traffic to and from that server should be protected by a firewall.

The Information Technology Department will be required to configure firewalls in such a way as to ensure that only the minimum required traffic is allowed through the firewall.

5.11 Software

Only licensed copies of approved commercial software will be installed on Trust equipment. It is a criminal offence to make or use unauthorised software and users of such will face disciplinary action.

5.12 Virus Protection

All Trust computers, laptops and servers will be protected with anti virus software.

Staff must report any detected or suspected viruses to the Information Technology Department immediately.

5.13 Information Security Incidents - including Cyber Security incidents

A security incident is any of the following: -

- Loss or theft of Trust equipment
- Loss or theft of data / information
- Unauthorised access to information \ systems
- Threat to the security of the Trust Network either by introduction of virus's or other malware and or disruption to service provision

All information security incidents must be reported immediately via the Trust's Incident Reporting Policy. The Head of Information Security and the Head of Information Governance must also be informed.

5.14 Business Continuity and Disaster Recovery

The Trust will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

6. Consultation

This policy was developed in consultation with the Information Governance Group and all staff via the Intranet.

7. Implementation

This policy will be implemented through the day to day management of systems/Networks through the Information Technology Department.

Staff awareness of information security will be raised through Information Governance training sessions.

8. Training and Support

Information security will be included in the Information Governance Corporate Induction and Awareness Training to staff as identified on the Trust's Training Needs Analysis.

9. Review

This policy will be reviewed at least every 3 years by the policy author.

10. Monitoring Compliance

MONITORING COMPLIANCE WITH THE DOCUMENT					
Aspect of compliance or effectiveness being monitored	**Monitoring method**	**Individual / Department responsible for the monitoring**	**Frequency of monitoring activity**	**Group / Committee which will receive the findings / monitoring report**	**Group / Committee / Individual responsible for ensuring that the actions are completed**
Compliance with information security (will be done via exception reporting of breaches / loss or information or equipment)	Performance Dashboard	Information Governance	Quarterly	Information Governance Group	Information Governance Group
Cyber Security Threats	Ongoing software to detect and deflect attack	Information Technology Department	Continual programmes – execption reports monthly	Information Governance Group	Information Governance Group

11. References

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Copyright Designs & Patents Act 1988
- The Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000
- Data Retention and Investigatory Powers Act 2014
- The NHS Information Governance Assurance Statement

12. Trust Associated Documents

- Email Usage Policy
- Internet Usage Policy
- Laptop Usage Policy
- Removable Media/Devices Policy
- Safe Haven Policy
- System Level Security Policy
- Incident Reporting Policy

13. Version Control

Version	**Date**	**Author** (name and designation)	**Status** (Draft/Approved)	**Comments**
V1.0		Naomi Wills Head of Information Governance		
V2.0		Naomi Wills Head of Information Governance		
V3.0		Naomi Wills Head of Information Governance	Approved	Approved
V4.0	Sept 09	Naomi Wills Head of Information Governance	Draft	Reviewed as part of 2 yearly review and following Audit recommendations
V4.0	Oct 09	Naomi Wills Head of Information Governance	Final	Approved and Ratified
V4.1	July 12	Naomi Wills Head of Information Governance	Approved	Expiry date extended for 4 months.
V5.0	Sept 12	Becky Keough NHSLA Co-ordinator	Draft	Full Review
V5.1	26/10/12	Naomi Wills Head Of Information Governance	Approved/ratified	Approved/ratified by the Policy Review Group
V6.0	04/01/16	Naomi Wills Head of Information Governance	Approved	amendments to titles and documents – inclusion of cyber security

14. Equality Impact Assessment

DOCUMENT / PROJECT NAME: Information Security Policy			
		Yes / No	**Comments**
1.	**Does the document affect one group less or more favourably than another on the basis of: -**		
	Race	NO	
	Human Rights	NO	
	Gender (inc gender reassignment)	NO	
	Religion or Belief	NO	
	Sexual Orientation	NO	
	Age	NO	
	Disability (learning disabilities, physical disability, sensory impairment and mental health)	NO	
2.	**Is there any evidence that some groups are affected differently?**	NO	
3.	**If you have identified potential discrimination are there any expectations valid, legal and / or justifiable?**	N/A	
4.	**Is the impact of the document / guidance likely to be negative?**	N/A	
5.	**If so, can the impact be avoided?**	N/A	
6.	**What alternative is there to achieving the document / guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different actions?**	N/A	
8.	**How has the consultation taken place and who with?**	YES	**Who with:** Information Governance Committee and Trustwide via the Intranet
9.	**EIA Team:** 3 people who contributed to this assessment	**1.** Naomi Wills, Head of Information Governance **2.** Becky Keough, Risk and Compliance Coordinator **3.** Paul Masters, Assistant Director Governance	
10.	**Date of the Assessment:**	04/02/2016	

If you have identified a potential discriminatory impact on this procedural document, please refer it to the author of the policy or strategy, together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please refer to the guidance notes.

Please return to the Equality and Diversity Department