Wirral Clinical Commissioning Group

ICT SECURITY POLICY

Version	**1.0**
Ratified By	**Governing Board**
Date Ratified	**5th March 2013**
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	**5th March 2013**
Review Date	**5th March 2014**
Intended Audience	**All CCG Employees**
Impact Assessed	**Yes**

This policy covers the following organisations:

- NHS Wirral Clinical Commissioning Group
- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group

Further information about this document:

Document name	**ICT Service Security Strategy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Mark Bakewell** **Chief Finance Officer**
This document should be read in conjunction with	**All other ICT Service policies**
Published by	**NHS Wirral Clinical Commissioning Group supported by** **Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU** **Main Telephone Number: 0844 800 9982 (Freephone)**
Copies of this document are available from	Website: www.wirralccg.nhs.uk/About%20Us/ourpolicies.htm or NHS Wirral Clinical Commissioning Group, Old Market House, Hamilton Street, Birkenhead, Wirral, CH41 5AL

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

Table of Contents

1.0 Policy Statement

This top-level information security policy should be considered as a key component of the organisation's overall information security management framework and should be considered alongside more detailed information security documentation.

2.0 Organisational Responsibilities

2.1 CCG Board

The Chief Operating Officer is responsible for this Policy.

2.2 CCG Committee which includes Information Governance in the Terms of Reference

The committee is responsible for ensuring this policy is implemented in partnership with the Cheshire ICT Service and that systems and processes are developed and monitored.

2.3 Managers

Managers and Supervisors are responsible for ensuring that all staff are aware of their responsibilities under the Policy and that it is fully implemented throughout their department.

2.4 Employees, Volunteers, Contractors, sub-contractors

All staff, whether clinical or administrative, who have access to ICT systems, have a responsibility to ensure compliance with this policy.

3.0 Planning and Implementation

3.1 This policy will be approved and ratified by the CCG Committee which includes Information Governance in the Terms of Reference

3.2 All Managers will have access to this policy via the organisation's Internet site

3.3 There are no formal training requirements for this policy although general ICT training is available via the Cheshire ICT Service

4.0 Policy

The objectives of the information security policy are 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

4.1 Management of Security

At board level, responsibility for Information Security shall reside with the Senior Information Risk Officer (SIRO).

Cheshire ICT Service's Information Security Team shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

4.2 Information Security Awareness Training

Information security awareness training should be included in the staff induction process.

An ongoing awareness programme should be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

4.3 Contracts of Employment

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

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

4.4 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

4.5 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

4.6 User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

4.7 Computer Access Control

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

4.8 Application Access Control

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.

4.9 Equipment Security

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

4.10 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Information Security Management Group.

4.11 Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the organisation's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

4.12 Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Cheshire ICT Service's Service Desk on 0844 800 9982. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

4.13 Classification of Sensitive Information.

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

The classification **NHS Confidential** – shall be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies. In order to safeguard confidentiality, the term "NHS Confidential" shall **not** be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice. Documents so marked shall be held securely at all times in a locked room to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Documents marked NHS Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

The classification **NHS Restricted -** shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or it's officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;

- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.
- NHS Restricted documents should also be stored in lockable cabinets

4.14 Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat 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 Cheshire ICT Service. Users breaching this requirement may be subject to disciplinary action.

4.15 User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the organisation before they may be used on their corporate systems. Such media must also be fully encrypted and virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

4.16 Monitoring System Access and Use

An audit trail of system access and data use by staff (where available) shall be maintained and reviewed on a regular basis.

The organisation has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right 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

4.17 Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the SIRO before they commence operation.

4.18 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the organisation.

4.19 Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Cheshire ICT Service. Users shall not install software on the organisation's property without permission from the Cheshire ICT Service. Users breaching this requirement may be subject to disciplinary action.

4.20 Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

4.21 Reporting

The Information Security Team shall keep the SIRO informed of the information security status of the organisation by means of regular reports.

5.0 Measuring Performance

5.1 This policy will be reviewed every 12 months

5.2 The number of incidents relating to information security will be monitored and reviewed

5.3 Number of communications that raise awareness of this policy and associated issues.

6.0 Audit

Where internal audit are carrying out work that includes polices relating to Information Communications Technology or Information Governance then this policy will be audited.

7.0 Review

This policy will be reviewed 12 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.