NHS
Hambleton, Richmondshire and Whitby
Clinical Commissioning Group

INFORMATION SECURITY POLICY

Authorship:	Chris Wallace – Information Governance Manager
Committee Approved:	Quality and Clinical Governance Committee
Approved date:	December 2014
Review Date:	Jan 2016
Equality Impact Assessment **Sustainability Impact Assessment** **Target Audience:**	Screening Completed All Staff
Policy Reference No:	N/A
Version Number:	1.1

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.2	Chris Wallace	First draft for comments		
1.0	Barry Jackson	Approved version		
1.1	IG Team	To add guidance re encryption and cloud storage	DECEMBER 2014	

CONTENTS

1 INTRODUCTION

Information and information systems are important assets to every organisation and it is essential to take all the necessary steps to ensure that they are comprehensively protected, available and accurate to support the operation and continued success of the CCG at all times.

The Information Security Policy is a key component of the CCGs overall information security management framework and is designed to:

- provide a corporate framework in which security threats to our Information Systems can be identified and managed;
- illustrate the CCGs commitment to the security information and information systems;
- provide accepted formal procedures to ensure a uniform implementation of security measures;
- introduce and formalise procedures to minimise the risk of unauthorized modification, destruction or disclosure of information; and
- align the organisation to the NHS Information Governance aims and expectations described in the Information Security Management: Code of Practice for NHS Organisations.

Note: these objectives can only be achieved if every staff member observes the highest standards of personal, ethical and professional conduct in relation to the handling and management of information.

1.1 Requirement for Security Policy.

The CCG acknowledges that information is a valuable asset, therefore it is within its interest to ensure that the information it holds is suitably protected from any threat. By protecting its information the CCG is acting in the best interests of its employees and all third parties with whom information is shared whilst minimising key risks associated with information processing:

- legal action due to non-compliance with statutory and regulatory requirements
- loss of public confidence in the CCG
- contribution to clinical or corporate negligence

Key issues addressed by the Security Policy are:-

- Availability - information is delivered to the right person when it is needed.
- Confidentiality - data access is confined to those with specified authority to view the data;
- Integrity - all system assets are operating correctly according to specification and in the way the current user believes them to be operating; and

The CCG intends to achieve a standard of excellence in Information Governance by ensuring all information is dealt with legally, securely, efficiently and effectively in order to support the delivery of high quality patient care, service planning and operational management. For this to be achieved information processing must comply with legislation and best practice and the CCG will establish and implement policies and procedures to ensure appropriate standards are defined, implemented and maintained.

1.2 Legal Compliance

The CCG is bound by the provisions of a number of items of legislation affecting the stewardship and control of patient and other information. The main relevant legislation is:

- The Data Protection Act 1998;
- Access to Health Records Act, 1990 (where not superseded by the Data Protection Act, 1998);
- Computer Misuse Act, 1990;
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998; and
- The Human Rights Act 1998.

This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected. In addition to the above, other legislation can impact upon the way in which we should use personal information. This includes:

- Public Interest Disclosure Act 1998;
- Audit & Internal Control Act 1987;
- Public Health (Code of Practice) Act 1984;
- NHS (VD) Regulations 1974;
- National Health Service Act 1977;
- Human Fertilisation & Embryology Act 1990;
- Abortion Regulations 1991;
- The Terrorism Act 2000;
- Road Traffic Act 1988;
- Regulations under Health & Safety at Work Act 1974.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.

Much of the legislation mentioned is available in electronic format, via the Internet (www.legislation.hmso.gov.uk). In addition, the CCG is bound by the confidentiality aspects of common law and the Caldicott guidance on protection of patient information.

As part of, and in addition to, the above legislation the CCG is required to retain all records (health and administrative) for specified periods of time. For further information on this see the Records Management Policy.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc

5 POLICY PURPOSE & AIMS

Operating Procedures and Standards

5.1 Compliance

It is the policy of the CCG to ensure compliance, in accordance with all the legislative obligations. The CCG also requires all employees, contractors and third parties to comply with this policy and supporting standards and procedures where appropriate.

5.2 Information Security Awareness and Education

It is the responsibility of all employee's and third parties of the CCG to sustain excellent information security. To comply with this, the CCG requires all employees and contractors within scope to understand the importance of information security and be familiar with this document, and supporting documents where appropriate.

To facilitate this information governance training will be included in the staff induction process and as an annual requirement in order to ensure staff awareness is refreshed and updated as necessary.

5.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. In addition information security expectations of staff shall be included within appropriate job definitions.

5.4 Email and Electronic Systems

The CCG has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The procedures cover use of any systems used to store, retrieve, manipulate and communicate information (e.g. telephone, fax, e-mail, IT systems and the Internet). All employees and third parties are required to familiarise and adhere to them.

5.5 Access Controls

Physical Security:

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

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

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

Devices which have not been issued by the CCG must not be connected to CCG equipment, e.g. personal mobile phones, I-pods, etc. as they could introduce viruses which could corrupt or destroy CCG information held within the network.

User Access Controls:

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

Computer Access Controls:

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

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.

The CCG has a procedure outlining the control of access to its premises, physical assets and electronic networks. Procedures also cover correct use of its assets. All

employees and third parties are required to acquaint themselves with these standards.

5.6 Computer and Network Procedures

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

5.7 Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the Information Asset Register and action plans shall be put in place to effectively manage identified risks. The Information Asset Register and all associated action plans shall be reviewed quarterly by Information Asset Owners. Any implemented information security arrangements shall also be a regularly reviewed feature of the CCGs 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.

5.8 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported via the CCGs Incident Management process to the Head of IMT.

All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.9 Classification of Sensitive Information – [Pending New Guidance]

The CCG will implement information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their NHS information assets. For more information on information classification is contained within the CCG Records Management Standard and Procedures.

5.10 Protection from Malicious Software

The CCG will 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 will not install software on the CCGs property without permission from the Head of IMT. Users breaching this requirement may be subject to disciplinary action.

5.11 User Media

The CCG will use port control software to control the use of removable media. Access to USB mass storage devices and CD/DVD writers will be restricted to approved users only.

Where removable media is received from external sources or has been used on computers systems not owned by the CCG users are required to scan the media using anti-virus software before its use.

All removable magnetic media must be encrypted. Failure to do this may result in disciplinary action.

5.12 Encryption

Following Department of Health requirements all mobile computing equipment will be encrypted to ensure data security. This ensures if the device is lost or stolen only pre-approved user will be able to access and content stored locally.

To ensure data security on other media types, along with port controls described above, only encrypted removable media will be sanctioned for use. Any USB removable media will be required to meet UK eGovernment Interoperability Framework standards for encryption.

Where data of a personal confidential nature is to be written to CD or DVD media then this will also require encryption. The CSU will ensure software is made available to use that allows the encryption of data before it is copied to the disk.

5.13 Online or Cloud Storage

The use of online or cloud storage is prohibited and staff should not use any service that has not been provided through the CSU IMT department. Some device manufactories provide cloud based storage options with their products. If you setup your work supplied device or use your own device you will be responsible for ensuring that any data on the device does not synchronise with the cloud.

5.14 Accreditation of Information Systems

The CCG shall ensure that all new information systems, applications and networks include a security policy and are approved by the Head of IMT before implementation.

System specific security policies will be developed for systems under CCG control in order to allow granularity in the security management considerations and requirements of each. This may result in specific responsibilities being assigned and obligations communicated directly to those who use the system.

5.15 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Head of IM&T or authorised officer.

5.16 Intellectual Property Rights

The CCG shall ensure that all information products are properly licensed and approved by the Head of IMT.

Users shall not install software on the organisation's property without permission from the Head of IMT. Users breaching this requirement may be subject to disciplinary action.

5.17 Business Continuity and Disaster Recovery Plans

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

It is the responsibility of all employees and contractors to familiarise themselves, as appropriate, with the business continuity plan that supports this policy.

5.18 Reporting

The Head of IMT will keep the Executive Management Group informed of the information security status of the organisation by means of regular reports and presentations.

5.19 Policy Audit

This policy will be subject to regular independent audit and annual assessment in line with the completion of the Information Governance Toolkit by internal and external audit.

5.20 Physical Security

All staff are responsible for the physical security of assets, equipment and building used by the CCG. Appropriate physical security measures shall be put in place to secure information assets dependant on value and sensitivity to the organisation.

All staff are responsible for ensuring that buildings are left is a secure state when vacant.

5.21 Policy Violations

It is a condition of employment with the CCG that compliance should be maintained where appropriate with the information security management policy, and supporting standards and procedures.

If any procedures or policies are violated these will be treated as security incidents, and reported in accordance with the CCGs incident reporting procedure. Failure to comply with this policy, or supporting procedures, could result in disciplinary action.

6 ROLES / RESPONSIBILITIES / DUTIES

Information Security Responsibilities

Policy review and maintenance	Chief Finance Officer / SIRO
Approval	CCG Executive Management Team
Adoption	All manager, staff and contractors

Responsibility for Information Security will reside with the CCG Executive Management Team. On a day-to-day basis the Head of IMT will be responsible for implementing, managing, monitoring, documenting and communicating the security requirements for the organisation.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- the information security policies and procedures applicable in their work areas;
- their personal responsibilities for information security; and
- how to access advice on information security matters

All staff will comply with information security policies and procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Line managers will be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff will be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

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

7 IMPLEMENTATION

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

8 TRAINING & AWARENESS

Staff will be made aware of the policy via the Intranet

9 MONITORING & AUDIT

Monitoring System Access and Use

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

The CCG has in place routines to regularly audit compliance with this and other policies. In addition the CCG 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

10 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

11 REFERENCES

Supporting Documents and Procedures
The following documents are in support of the Information Security Policy:-

Confidentiality Policy

Network Security Policy

Records Management Policy

Monitoring Standards and Procedures

Appendix 1

1. Equality Impact Analysis	
Policy / Project / Function:	Information Security Policy
Date of Analysis:	13/01/14
This Equality Impact Analysis was completed by: **(Name and Department)**	C Wallace - IG Manager – CSU IG Team
What are the aims and intended effects of this policy, project or function ?	This standard documents the CCG's information security framework and security standards that are in place.
Please list any other policies that are related to or referred to as part of this analysis?	
Who does the policy, project or function affect ? Please Tick ✔	Employees ☒ Service Users ☐ Members of the Public ☐ Other (List Below) ☐

2. **Equality Impact Analysis: Screening**					
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact
	Yes	No	Yes	No	
Race	☐	☒	☐	☒	
Age	☐	☒	☐	☒	
Sexual Orientation	☐	☒	☐	☒	
Disabled People	☐	☒	☐	☒	
Gender	☐	☒	☐	☒	
Transgender People	☐	☒	☐	☒	
Pregnancy and Maternity	☐	☒	☐	☒	
Marital Status	☐	☒	☐	☒	
Religion and Belief	☐	☒	☐	☒	
Reasoning					
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7					

Appendix 2

SUSTAINABILITY IMPACT ASSESSMENT

Policy / Report / Service Plan / Project Title:				
Theme (Potential impacts of the activity)	**Positive Impact**	**Negative Impact**	**No specific impact**	**What will the impact be? If the impact is negative, how can it be mitigated? (action)**
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			X	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			x	
Reduce the risk of pollution and avoid any breaches in legislation.			x	
Goods and services are procured more sustainability.			x	
Reduce carbon emissions from road vehicles.			x	
Reduce water consumption by 25% by 2020.			x	
Ensure legal compliance with waste legislation.			x	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			x	
Increase the amount of waste being recycled to 40%.			x	
Sustainability training and communications for employees.			x	
Partnership working with local groups and organisations to support sustainable development.			x	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			x	