NHS
Barnsley Clinical Commissioning Group

Putting Barnsley People First

BARNSLEY CLINICAL COMMISSIONING GROUP'S INFORMATION SECURITY POLICY

February 2014

Version:	1
Approved By:	Governing Body
Date Approved:	13 February 2014
Name of originator / author:	Richard Walker
Name of responsible committee/ individual:	Governing Body (Approval) Information Governance Group (review)
Name of executive lead:	Vicky Peverelle
Date issued:	
Review Date:	2 years from approval
Target Audience:	Barnsley CCG staff

THIS POLICY HAS BEEN SUBJECT TO A FULL EQUALITY IMPACT ASSESSMENT

Amendment Log

Version No	Type of Change	Date	Description of change
DRAFT		January 2014	
1		13 February 2014	*Approved by Governing Body*

Information Security Policy

1. Introduction

1.1 The objective of information security is to protect the CCG's information assets[1] from a wide range of threats, whether deliberate or accidental, internal or external, in order to ensure business continuity and minimise the impact of adverse events on patients, staff and the CCG. Information security is achieved through the implementation of controls and procedures that ensure the secure use of information and the identification and effective management of risk. This policy should be cross-referenced with other information governance and procedural documents. An up to date list of documents is available on the information governance intranet page. Staff should ensure that they are familiar with the content of this policy.

2. Objectives

2.1 The purpose of this policy is to enable the CCG to protect its information assets by:

i. setting out a framework for information security;
ii. promoting a culture of information security within the CCG and
iii. ensuring staff understand their responsibilities in relation to information security.

2.2 The information security policy will ensure that:

- The CCG has a Governing Body approved Senior Information Risk Owner (SIRO)
- Each Information Asset has a responsible owner (Information Asset Owner)
- Information is protected against unauthorised access and/or misuse
- The confidentiality of information is assured[2]
- The integrity of information is maintained[3]
- Information is available when required
- Business continuity plans are produced, maintained and tested[4]
- Regulatory, legal and contractual requirements are complied with[5]

- Training around information security is provided to all staff
- All breaches of information security, actual or suspected are reported and investigated through the appropriate management channels (see section 4.8)

2.3 Controls and procedures will be produced to support this policy and implement the framework[6]

[1] Information takes many forms and includes data stored electronically and in hard copy, transmitted by any means, including by email, by fax, in spoken in conversation over the telephone or face to face, printed out or written as hard copy.
[2] Personal, valuable and sensitive information will be protected from unauthorised access and disclosure.
[3] Information will be protected against unauthorised modification and destruction.
[4] This will ensure that information and vital services are available to users when required.
[5] Including compliance with the Data Protection Act 1998, NHS Code of Connection, Copyright, Designs and Patents Act 1988, Computer Misuse Act 1990 and any other relevant legislation and regulations.
[6] These will be maintained as part of a suite of information governance policies and posted on the intranet.

3. Scope

This policy applies to the following areas:

3.1 Systems

- All manual and electronic information systems owned, operated or managed by the CCG, including networks and application systems, whether or not such systems are installed or used on CCG premises.
- Other systems brought onto CCG premises including, but not limited to, those of contractors and 3rd Party suppliers, which are used for CCG business.

3.2 Users

- All users of CCG information and/or systems including CCG employees and non-CCG employees who have been authorised to access and use such information and/or systems.

3.3 Information

- All information collected or accessed in relation to any CCG activity whether by CCG employees or individuals and organisations under a contractual relationship with the CCG.
- All information stored on facilities owned or managed by the CCG or on behalf of the CCG.
- All such information belongs to the CCG unless proven otherwise.

4. Framework for Information Security

4.1 Management of, and Responsibility for, Information Security

- The Accountable Officer has ultimate responsibility for information security within the CCG. This is delegated to the Senior Information Risk Owner.
- The CCG's Senior Information Risk Owner is responsible for implementing, monitoring, documenting and communicating information security requirements for the CCG.
- Departmental and line managers are responsible for information security within their area or work and for ensuring their staff[7] are aware of this policy and associated procedures and their duty to comply. They must ensure all their key information assets have an identified responsible owner (Information Asset Owner).
- Information Asset Owners are responsible for identifying and managing the risks associated with their asset.
- Individuals have a personal responsibility for adhering to this policy and associated information governance procedures.
- Failure to comply with the policy and associated procedures may have serious consequences for the individual including civil, criminal and disciplinary proceedings.

4.2 Contracts of Employment

- Security requirements are addressed at the recruitment stage and all contracts of employment contain a clause relating to confidentiality and data protection.

[7] This includes all individuals for whom the manager is responsible including but not limited to: permanent and temporary staff, staff on secondment, contractors, students on placement, volunteers etc.

4.3 Information Security Awareness Training

- Information security awareness training is included in the staff induction process.
- An on-going programme of awareness is established to ensure that staff awareness is refreshed and updated.
- The Senior Information Risk Owner and Information Owners are required to undertake mandatory training annually.

4.4 Information Security Procedures

- The security of paper and electronic records, computers and networks is controlled by procedures that have been authorised by the appropriate authority within the CCG, or WSYB CSU where the asset is provided under contract to, or managed on behalf of, the CCG.

  Areas of information security covered include, but are not limited to:

4.4.1 Security of Equipment and Records

- In order to minimise loss of, or damage to, all assets, all equipment and information storage areas are physically protected from security threats and environmental hazards.
- Confidential information held in hard copy (paper) must be kept secure at all times.
- Confidential CCG information must not be stored on local hard drives such as PCs, lap tops or other portable devices unless authorised by the Head of Assurance.
- Any confidential information held on portable devices must be encrypted.
- Databases of personal, that is, service user information and staff information, must not be created without prior permission from the Head of Assurance.
- Current databases of personal information must be notified to the Head of Assurance.

4.4.2 Location Access Controls

- Only authorised personnel who have an identified need are given access to restricted areas containing information systems such as the server room.

4.4.3 User Access Controls

- Access to information and information systems, whether electronic or manual, is restricted to authorised users who have an identified need as agreed with their line manager or sponsor.
- Access to electronic information systems is given at the appropriate level for the agreed need.
- Person confidential data may only be stored within operational systems or within a safe haven.

4.4.4 Information Communication Technology (ICT) Access Controls

- Access to ICT equipment, for example, PCs and terminals is restricted to authorised users who have an agreed requirement to use those facilities.

4.4.5 Connection to the CCG Network

- All devices connected to the CCG network are governed by the Statement of Compliance.

- The connection of any equipment to the CCG network requires authorisation from the IT department.
- All electronic processing devices connecting to the CCG network must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that the anti-virus software is up to date.

- Personally owned devices must not be directly connected to the NHS Barnsley Clinical Commissioning Group (the CCG) network.
  - Directly connected means either by wire (network cable) or wifi.
  - The CCG network means Library or personal drives, database or intranet
  - Personally owned means devices that are not provided by the CCG or other NHS organisation.
  - Devices includes home personal computers, laptops, tablet computers (for example, ipads), media players (such as ipods) and smart phones.
  - An exception is PDAs, which may be connected to your PC via a USB port in order to synchronise diaries. This requires prior authorisation of the IT Service Desk.
- The CCG has the facility to allow non-NHS provided devices to connect to the internet via a wireless connection. This should be authorised by the IT Department - Ask the IT Service Desk for advice.
- External visitors may connect to the internet via a Guest wifi account.

4.4.6 Remote Working

- Information that is taken off site must be authorised by line management, protected by proper security and, where held on portable computers, backed up regularly. Portable devices must be used in line with CCG policy and protected by appropriate security (See Remote Working and Portable Devices Policy). Working from home must be authorised

  by line management and comply with policies relating to information governance and home working.

4.4.7 Portable Devices

- The use of portable devices for work purposes must be in line with CCG policy and authorised by your line manager (and Information Governance/IT Services where appropriate). (See Remote Working and Portable Devices Policy)
- Only portable devices that have been provided / authorised for use by IT Services may be used for work purposes. This includes, but is not limited to, laptops, tablets such as ipads, USB sticks, digital dictation machines, smart phones.
- Personally owned portable devices such as laptops and ipads must not be directly connected to the NHS Barnsley Clinical Commissioning Group network either by wire (network cable) or wifi (refer to section 4.4.5 above)
- The CCG has the facility to allow non-NHS Barnsley Clinical Commissioning Group provided portable devices to connect to the internet via a wireless connection. (refer to section 4.4.5 above).
- Portable storage devices (including CDs, DVDs and flash drives) containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on CCG equipment and must be protected by proper security (Ask IT Service Desk for advice).

- All portable devices must be protected by appropriate security. Portable devices such as laptops, tablets (for example, ipads), dictation machines smart phones and USB sticks must be encrypted and, where appropriate, have up to date anti-virus software.
- Portable devices used to access NHS mail must be encrypted and have the capacity, and be configured, to allow remote wiping.

4.5 Malicious and Unauthorised Software

- The CCG will use countermeasures and management procedures to protect itself against the effects of malicious software. All staff are expected to co-operate fully with this requirement.

- Users must not install software on CCG equipment without permission from the IT Support Desk.

4.6 Monitoring System Access and Use

- Audit trails of system access and use are maintained and reviewed on a regular basis.

4.7 Business Continuity

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

4.8 Reporting Security Incidents and Weaknesses

- All information management and technology security incidents and weaknesses must be reported via CCG incident reporting procedures.
- Incidents that present an immediate risk to the CCG such as viruses should be reported to the IT Service Desk immediately.

4.9 Reporting to the Information Governance Group

- The Head of Assurance will keep the Senior Information Risk Owner, Information Governance Group and/or Quality and Patient Safety Committee informed of the information security status of the CCG by means of regular reports.

5. Legislation and Guidance

- The CCG and its employees, including non-CCG employees authorised to access CCG information and systems, are obliged to comply with the legislation and national guidance including, but not limited to:

  - Common Law Duty of Confidentiality
  - Data Protection Act 1998
  - Computer Misuse Act 1990
  - Freedom of Information Act 2000
  - Protection of Freedoms Act 2012

  - Health and Social Care Act 2012
  - Regulation of Investigatory Powers Act 2000
  - Copyright, Designs and Patents Act 1998
  - Statement of Compliance
  - Confidentiality: NHS Code of Practice

- Records Management: NHS Code of Practice
- Information Security: NHS Code of Practice

And any relevant guidance related to the following:

- Information Quality Assurance
- Information Security
- Information Governance Management
- National systems

6. Further information

- Further information can be obtained from the CCG's Information Governance Lead.
- Questions about the use of portable devices or any problems in accessing the CCG system should be directed to the IT Service Desk. Support is available during opening hours. There is no out of hours or home support.

Equality Impact Assessment 2013

Title of policy or service	Information Security	
Name and role of officers completing the assessment	Julie Eckford, IG Specialist	
Date assessment started/completed	21.01.14	21.01.14

1. Outline

Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	The policy aims to raise CCG staff awareness of the CCG's expectations in relation to the appropriate handling of information when using the internet to: • Ensure information is handled appropriately and in a secure and confidential manner • Reduce the risk of adverse incidents • Prevent staff inadvertently causing an IG incident through non-compliance of CCG policy The policy links to law such as data protection law, guidance issued by organisations such as DH, Information Commissioner's Officer and Cabinet Office, ISO security standards and other CCG IG policies including email, internet and the confidentiality code of conduct.

2. Gathering of Information

This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			What action do you need to take to address these issues?	What difference will this make?
	Positive	**Neutral**	**Negative**		

	Impact	impact	impact		
Human rights		Y			
Age		Y			
Carers		Y			
Disability		Y			
Sex		Y			
Race		Y			
Religion or belief		Y			
Sexual orientation		Y			
Gender reassignment		Y			
Pregnancy and maternity		Y			
Marriage and civil partnership (only eliminating discrimination)		Y			
Other relevant group		Y			

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	The EIA will be reviewed when the policy is reviewed. The Head of Assurance is responsible for ensuring the review takes place. This policy will be reviewed not later than 2016.		
Lead Officer	Richard Walker	**Review date:**	13 February 2014