NHS

Bolton Clinical Commissioning Group

# Corporate Information Security Policy

| | |
|---|---|
| **Policy Number** | **IG003** |
| **Target Audience** | **CCG/GMSS Staff** |
| **Approving Committee** | **CCG Executive** |
| **Date Approved** | **February 2016** |
| **Last Review Date** | **Jan 2016** |
| **Next Review Date** | **Jan 2019** |
| **Policy Author** | **IG Manager (GMSS)** |
| **Version Number** | **V4.0** |

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

## Version Control Sheet

| Version | Date | Reviewed By | Comment |
|---|---|---|---|
| 1 | August 2013 | M Robinson<br>D Sankey | Approved by CCG Executive team |
| 2 | November 2013 | Andrea Hughes | Inserted paragraphs 3.9-3.12 (approved at exec) |
| 2.1 | June 2015 | IG | Reviewed & progress to IM & T Operations Board for approval. |
| 2.2 | June 2015 | IM & T Operation Board | Approved |
| 3.0 | Jan 2016 | IG Team | Reviewed |
| 3.1 | Feb 2016 | IM & T Operation Board | Approved |
| 4.0 | Nov 2016 | IG Team | Reviewed |
| 4.1 | Dec 2016 | IM & T Operations Board | **Reviewed and approved.**<br>**CO final sign off** |

| | | |
|---|---|---|
| Analysis of Effect completed: | By: M Robinson | Date: August 2013 |

Contents Page

# 1 Introduction and Aims

1.1 The information held and managed by the CCG is an asset that all staff have a duty and responsibility to protect. The availability of complete and accurate information is essential to the CCG functioning in an efficient manner.

1.2 The aims and objectives of the CCG Corporate Information Security Policy is to set out a framework for the protection of the organisation's information.

1.3 The objectives of this policy are to ensure the security of the CCG assets, primarily:

- To ensure availability that assets are available as and when required hence adhering to the organisation's business objectives.
- To preserve integrity to protect assets from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets.
- To preserve confidentiality to protect assets against unauthorised disclosure.

1.4 The aims of the policy are to:

- protect against threats, whether internal or external, deliberate or accidental;
- enable information sharing in a secure and consistent manner;
- encourage consistent and secure use of information;
- ensure all users of information have a clear understanding of their roles and responsibilities in the protection and use of information;
- ensure the continuity of IT Services and minimise disruption to business operations;
- ensure the CCG meets its legal and regulatory responsibilities.

1.5 The CCG Corporate Information Security Policy is a high-level document that utilises a number of controls to protect the organisation's information. The controls are delivered through policies, processes and procedures, supported by tools and user training.

# 2 Scope

2.1 This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

2.2 The CCG Corporate Information Security Policy applies to all forms of information, including but not limited to:

- information stored in manual filing systems;
- communications, including those sent by post, courier, electronic mail, text messaging and bluetooth;
- information that is stored in and/or processed by information systems including servers, personal computers (PCs), laptops, mobile phones, tablet devices, personal digital assistant (PDA) and any other mobile device that is allowed access to the CCG information systems and information;
- information that is stored, copied, moved or transferred to any type of removable or portable media such as, but not limited to, CDs, DVDs, tapes, USB devices (any type), memory sticks; and
- transmission of or passing information to third parties or others that are external to the CCG.

# 3 Principles

The CCG will undertake risk assessments to identify, quantify and prioritise information security risks. Controls will be selected and implemented to mitigate the risks identified.

Risk assessments will be undertaken using the Governments Risk Assessment methodology to identify and estimate the magnitude of risks and in accordance with the CCG Information Risk Policy.

## 3.1 **Information security – Requirements**

The CCG will implement technical and operational standards, policies and processes that align with prevailing standards such as ISO27001 (Information Security Management).

The requirements of policy, processes and procedures will be incorporated into the CCG operational procedures and contractual agreements

Information stored and processed by the CCG will be appropriate to business requirements and no information will be stored or processed unnecessarily.

Business continuity plans will be developed, implemented, maintained and tested and such plans will be a contractual obligation of any relevant supplier.

All breaches of information security, actual or suspected will be reported and suitably investigated in line with information incident management procedures which will provide guidance on what constitutes an information incident.

Training and education regarding information security will be given to staff, contractors and third parties as well as any others who will have access to CCG information and information systems.

## 3.2 Information security responsibilities

The Associate Director of Integrated Governance and Policy, is the designated owner of the Corporate Information Security Policy, responsible for the maintenance and update, ensuring timely review and approval and ensuring supporting policies, standards, processes and procedures are in place.

Heads of departments and line managers are responsible for ensuring all staff, contracted third parties (whether individual or an entity) are made aware of and comply with the Corporate Information Security Policy including supporting policies, standards, processes and procedures.

Responsibilities will be assigned and policies, processes and procedures for the management, operation and on-going security and availability of all data and information processing facilities will be implemented.

Appropriate controls will be applied to all types of communication, internal and external, to ensure the communication is secure, appropriate and reaches the intended recipient.

## 3.3 Asset management

All CCG information (electronic and hardcopy), software, computer and communication equipment and service utilities, will be accounted for and have an owner.

The CCG will implement controls that will ensure its assets are appropriately protected.

Owners of such assets owners will be responsible for the maintenance and protection of assets they are assigned.

## 3.4 Asset Management

Restricted information will be physically protected from unauthorized access, damage, interference and/or alteration.

Access to CCG information and information systems will be controlled, with access driven by business requirements.

Staff will be granted to CCG information systems and information based on their role and to a level that will enable them to carry out their job responsibilities.

A formal and documented user provisioning process will be implemented which will govern access to CCG information and information systems.

### 3.5 Information systems acquisition, development and maintenance

Information security requirements will be defined and communicated during the development of business requirements for new systems or changes to existing systems. Failure of the CCG constituent businesses to engage with IT, to define these requirements, will result in rejection of new systems or changes to existing systems.

Controls to mitigate risks identified during design, procurement, development, testing and deployment will be implemented.

### 3.6 Information security incident management

The CCG will develop and implement a formal incident reporting and escalation process.

All staff contractors and third parties will be made aware of procedures for reporting security incidents or vulnerabilities that may have an adverse impact on the security, integrity or availability of the CCG information and information systems.

Information security incidents and vulnerabilities associated with information systems will be reported within an agreed timeframe and prescribed corrective action taken.

### 3.7 IT service continuity management

A business continuity management process will be implemented to minimise the impact of a disruption of service and to recover from the loss of information assets.

The CCG will ensure arrangements are in place to protect critical business process from the effects of major failures or disasters, of information systems or services, and to ensure timely resumption.

### 3.8 Compliance

The CCG will abide by any law, statute, regulatory and/or contractual obligations affecting its information and information systems.

The design, operation, maintenance, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.

All staff, contractors and third parties and all others that are, or have been, authorised to access are required to comply with the Information Security Policy and its' supporting standards, policies, processes and procedures.

Failure to comply could result in disciplinary and/or legal action.

## 3.9 User Access Controls

Only authorised CCG staff or authorised support personnel are permitted to access CCG computers and the information that is held on them.

All CCG Staff must have their own unique computer account and only login to systems or applications that they have been granted access to.

Access controls must take account of security requirements of the business application and permit access to be granted only on approval by the system administrator in consultation with the appropriate senior manager where there is any concern or doubt.

Remote access to the CCG network is protected by strong authentication and passwords.

Employees will normally be granted access only to such information that is required to perform their work duties. If they are erroneously granted any other access, then this fact must be reported to their line manager immediately as it may become construed as unauthorised access.

Where information is copied between systems within the network, then employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the sender.

## 3.10 Passwords

Only the person to whom a password is issued should use that password and it must not be divulged to anyone else. Any doubts or exceptional circumstances that require disclosure must be referred to the local Greater Manchester Shared Service (GMSS) Information Governance Team immediately.

If you suspect that your password is known by another user you must change it as soon as possible. If a Systems Administrator is required to do this then it is up to the staff concerned to contact them.

Passwords used within the CCG's systems must be a minimum of 6 characters. All staff must change their password when prompted.

## 3.11 Encryption

Encryption is the process of converting information using an algorithm to make the information unreadable to anyone except those who have the decryption key.

The CCG will ensure all of its electronically held data is adequately protected from loss and inappropriate access.

To reduce the risk of unauthorised access the CCG will ensure that the following devices are encrypted by default:

- Laptops
- Open access Desktops
- Handheld devices (where windows OS is used)
- Portable storage devices (Memory sticks etc)
- Removable media e.g. Floppy disks, DVDs and cds.

Staff must not bypass, cause to bypass or use tools or software to bypass the encryption software installed on devices.

Guidance from the Department of Health and Health& Social Care Information Centre (HSCIC) specifies standards for encryption and a national procurement has taken place to provide the products to achieve these standards.

The CCG will ensure that all data stored on the above devices will be encrypted to a minimum of 256bit encryption. The software, processes and procedures to allow this are being implemented throughout the CCG via GMSS IT Services.

### 3.12 Anti-Virus

Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, Trojans and worms. Virus threats are a day to day threat, however the type, strain, and number of incidents may well increase due to the increase in web activity. This can cause serious disruption to both the user and IT Services.

- All CCG must computers run anti-virus software which is constantly updated.
- CCG Staff must contact the GMSS IT Service Desk if a virus incident is known or suspected.

### 3.13 Removable Media

Corporate IT systems automatically encrypt removable media. Removable media that contain software require the approval of the IT Helpdesk before they may be used on CCG systems. Users breaching this requirement may be subject to disciplinary action.

### 3.14 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. 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
- 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 IM&T Programme Group before they commence operation.

### 3.15 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the IM&T Programme Group e.g. removal or insertion of new systems.

## 4 Accountability, responsibilities and training

### 4.1 Chief Accountable Officer

Information Security is everyone’s business although responsibility resides ultimately with the Chief Accountable Officer but this responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO) and Information Security Officer as required by the Information Governance Toolkit.

### 4.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for information risk within the CCG and advises the Board on the effectiveness of information risk management across the Organisation.

### 4.3 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 within their team.
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters.

### 4.4 **Information Security Officer**

The Information Security Officer will:

- Hold a relevant qualification in Information Security.
- Have lead responsibility for information security management within the CCG acting as a central point of contact on information security for Staff.
- Monitor potential and actual security breaches.
- Ensure compliance with relevant legislation and regulations.

In carrying out these tasks the Information Security Officer will work closely with the IG team and IT Team.

In the first instance of an Information Security query then contact is to be made with the CCG lead.

### 4.5 **All 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 organisation.
- Their responsibility for raising any information security concerns with the IG Team.

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.

4.6 Overall responsibility for the Information Security Policy lies with the Information Security Manager (GMSS) who has delegated responsibility for managing the development and implementation of technical and operational procedural documents to IT Services and Line Managers.

4.7 Staff will receive training regarding the policy from a number of sources:

- specific training course;
- policy/strategy and procedure manuals;
- line manager;
- other communication methods (e.g. Team Brief/team meetings);
- intranet; and
- information governance toolkit training.

All individuals will be required to comply with this policy whilst working within the CCG.

All staff are mandated to undertake the "Introduction to Information Governance" e-learning module. Information Governance training is required to be undertaken on an annual basis.

## 5 Monitoring and review

5.1 This policy will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit

5.2 This Policy will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

## 6 Legislation and related documents

Information will be stored and defined in accordance with the Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and The Computer Misuse Act 1990.

## 7 Other relevant Procedural Documents

A set of Procedural Documents will be made available via the CCG Intranet.

- IG009 Confidentiality Audit Procedure
- Incident Management Procedures
- IG012 Secure Transfer of Information Procedure

This list is not exhaustive

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff intranet**.**