Bolton Clinical Commissioning Group

Corporate Information Security Policy

Policy Number	**IG003**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**December 2019**
Last Review Date	**October 2019**
Next Review Date	**October 2021**
Policy Author	**IG Team**
Version Number	**5.1**

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 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	Nov 2016	IM & T Operation Board	Approved
4.2	Sept 2019	IG Team	Reviewed and updated
5.0	Oct 2019	IG Board	Approved
5.1	Dec 2019	CCG Chief Officer	Approved

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

Contents Page

1 Introduction

Information processing is a fundamental part of Bolton CCG's purpose. It is important, therefore, that the CCG has a clear and relevant Information Security Policy. The CCG has a responsibility to comply with data protection and other legislation and ensure that organisational reputation is not damaged due to a lack of or ineffective information security policies and procedures.

This policy aims to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially it encompasses the behaviour of the people who manage information in the line of CCG business.

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.

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.

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

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.

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.

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

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.

This policy covers:

- All manual and electronic information systems owned, operated or managed by the CCG and its Information Technology provider (Bolton NHS Foundation Trust), 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 third party suppliers, which are used for CCG business.
- Desktop devices used to hold CCG information such as Laptops and PCs, tablets and mobile phones.
- Removable media, such as USB memory sticks and external hard drives.

3 Accountability and Responsibility

3.1 Chief Officer

Information Security is everyone's business although responsibility resides ultimately with the Chief Officer but this responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO), Head of IT and Cyber Security Lead as required by the Data Security and Protection (DSP) Toolkit.

3.2 Senior Information Risk Owner (SIRO)

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

3.3 Data Protection Officer (DPO)

As a public authority the CCG is required to appoint a Data Protection Officer by the General Data Protection Regulation (GDPR). The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the Chief Officer and directly to the Board in relation to data protection matters.

3.4 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.

3.5 Information Governance (IG) Manager

The Information Governance Manager will be responsible for maintaining appropriate policies and guidance for staff around the use and processing of personal data of information contained within CCG's information assets in line with data protection and data security legislation and regulations.

3.6 Head of IT and the Cyber Security Lead

The role of the Information Governance Manager is supported by the Head of IT and the Cyber Security Lead.

The Head of IT and the Cyber Security Lead are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure NHS England's systems and infrastructure remain compliant with the Data Protection Act 2018.

The Head of IT and the Cyber Security Lead are responsible for ensuring that all CCG electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

3.7 Information Asset Owners

Information Asset Owners are responsible for the maintenance and protection of assets they have been assigned and to ensure information is restricted to only those who require access to the information.

In addition they are required to check that third party data processors have appropriate ISO and/ or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties. Information Asset Owners are also responsible for ensuring appropriate data protection assurance from all third party suppliers processing CCG data. Information Asset Owners should liaise with the IG Manager, the Head of IT and the Cyber Security Lead if assistance is required.

3.8 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 CCG;
- Their responsibility for raising any information security concerns with the Head of IT and the Cyber Security Lead.

Contracts with external contractors that allow access to the CCG'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.

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 training.

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

All staff are mandated to undertake the “Information Governance” e-learning module, which incorporates information on Information Security. This training is required to be undertaken on an annual basis.

4 Policy Framework

4.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions and descriptions.

4.2 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.

4.3 Security Control Assets

CCG IT will establish an IT asset management process and associated system; this will involve support and collaboration from the Bolton NHS Foundation Trust IT department where applicable.

All IT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

4.4 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO. Users will be authorised CCG staff or authorised support personnel.

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 IAO and line manager where there is any concern or doubt.

Information saved on the network will be kept in a folder system per department and be restricted to those users who belong to that department.

Where Smartcard access is required, the relevant IAO and the CCG Registration Authority Sponsor will review whether access is necessary and the level of access that is required.

Users 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 access is required by a third party the IAO will need to be informed and assess whether access can be granted. The IAO should complete a risk assessment where control requirements are identified and agreed, particularly where the asset may contain personal data.

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

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

Where information is copied between systems within the network, then users 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.

4.5 Computer & Application Access Controls

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 license from the supplier.

4.6 Equipment Security

In order to minimise loss of, or damage to, all assets, the CCG IT Team along with Bolton NHS Foundation Trust IT's team shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

In addition:

- All central processors/networked file servers/network equipment shall be located in secure areas with restricted access;
- Local network equipment and network terminating equipment shall be located in secure areas/and or lockable cabinets;
- Equipment shall be protected from power supply failure where appropriate
- All equipment including PCs and laptops must be located in secure areas and/or secured to protect from theft.

4.7 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of the CCG.

4.8 Information Risk Assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risk assessments are performed at least annually to identify, quantify and prioritise information security risks. Guidance will be sought from the IG Manager and the Senior Information Risk Owner (SIRO).

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.

IAO's shall submit the risk assessment results, via the IG Manager, and associated mitigation plans to the SIRO for review. Controls will be selected and implemented to mitigate the risks identified.

4.9 Information Security Events and Weaknesses

All CCG information security events, near misses, and suspected weaknesses are to be reported to the Head of IT and the Cyber Security Lead or designated deputy and where appropriate reported as an Adverse Incident.

All adverse incidents concerning a breach in personal data shall be reported to the CCG's IG Manager and CCG's DPO. The CCG's Data Security & Protection Breaches / Incident Reporting Policy and Procedure must be complied with. Bolton NHS Foundation Trust's DPO may also be made aware of the incident if applicable.

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.

4.10 Classification of Sensitive Information

NHS England shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security and Protection (DSP) Toolkit to secure their information assets. Further details of the classifications controls can be found in the CCG's Records Management Policy.

4.11 Protection from Malicious Software

The CCG and its IT service provider, Bolton NHS Foundation Trust, shall use software countermeasures and management procedures to protect itself against the threat 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 computers run anti-virus software which is constantly updated.
- CCG Staff must contact the IT Service Desk if a virus incident is known or suspected.
- Users shall not install software on the organisation's property without permission from the Head of IT and the Cyber Security Lead and / or the Chief Technology Officer at Bolton NHS Foundation Trust.

All staff shall be expected to co-operate fully with this policy. Users breaching this requirement may be subject to disciplinary action

4.12 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 in association with their IT Provider, Bolton NHS Foundation Trust, 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
- Portable storage devices (Memory sticks etc)
- Removable media

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

4.13 Removable Media

Bolton NHS Foundation Trust IT systems automatically encrypt removable media. Removable media that contain software require the approval of the Head of IT and the Cyber Security Lead and / or the Chief Technology Officer at Bolton NHS Foundation Trust before they may be used on CCG systems. Users breaching this requirement may be subject to disciplinary action.

4.14 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The CCG and Bolton NHS Foundation Trust will put in place routines to regularly audit compliance with this and other policies. 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 and any other applicable law.

4.15 Passwords and Passphrases

Information / Cyber security experts now encourage the use of Passphrases. A passphrase is similar to a password in that they are used to control access to a computer system, program or data. Using a strong passphrase is the single most effective thing a user can do to prevent themselves and / or the CCG from experiencing a successful cyber attack

A passphrase is generally longer for added security and is sequence of words or other text which the user can normally relate to, a combination of memorability and security.

An example of a good ruleset would be:
- Three random words.
- The middle word is in uppercase.
- A number is placed before the three words and another is placed after
- Two special characters are placed at the end (!£$%^&*)

i.e. 1BoltonCYBEREngland19%£

Passphrases / Passwords used within the CCG's systems must use a complex pattern for IT network access and for IT applications and should be at least 10 characters.

Only the person to whom a passphrase / password is issued should use that passphrase / password and it must not be divulged to anyone else. Any doubts or exceptional circumstances that require disclosure must be referred to the Head of IT, the Cyber Security Lead and Information Governance Manager immediately.

If a user suspects that their passphrase / password is known by another user they 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.

All staff will be required to change their password when prompted.

4.16 Acquisition and Accreditation of Information Systems

The CCG along with their IT Provider, Bolton NHS Foundation Trust, shall ensure that all new information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the Head of IT, the Cyber Security Lead and the Chief Technology Officer at Bolton NHS Foundation Trust before they commence operation.

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, developments testing and deployment will be implemented.

4.17 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Head of IT, the Cyber Security Lead and the Chief Technology Officer at Bolton NHS Foundation Trust.

4.18 Business Continuity and Disaster Recovery Plans

The CCG along with their IT Provider, Bolton NHS Foundation Trust, will implement a business continuity management system (BCMS) that will 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.

Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

4.19 Training & Awareness

Data Security and Protection training is mandatory and all staff are required to complete annual on-line Data Security Awareness training. On induction all CCG staff are made aware of all Information Governance policies in particular the Data Security / Information Governance Staff handbook. Both the mandatory training and the handbook provide staff with guidance on IT protection.

4.20 IG requirements for New Processes, Services, Information Systems and Assets

The IG requirements for New Processes, Services, Information Systems and Assets procedure must be complied with when:

- A new process is to be established that involves processing of personal data (data relating to individuals);
- Changes are to be made to an existing process that involves the processing of personal data;
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data;
- Introducing any new technology that uses or processes personal data in any way.

Where personal data is concerned a Data Privacy Impact Assessment (DPIA) must be completed. This IG risk assessment must be completed before any new processes / changes are implemented. Advice should be sought from the IG Manager. The DPIA will be reviewed and assessed by the IG Board where approval must be granted before any implementation can begin.

5 Monitoring and review

This policy will be monitored through staff awareness and supporting evidence to the DSP Toolkit

This Policy will be reviewed on as per the review date, 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.

The Information Governance Manager with support from the Head of IT and the Cyber Security Lead is responsible for the monitoring, revision and updating of this document.

6 References and Legislation

- The Data Protection Act (2018)
- The General Data Protection Regulation
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2012)

7 Other relevant Procedural Documents

A set of Procedural Documents will be made available via the CCG Internet:

- Information Governance Policy
- Data Security & Protection Breaches / Incident Reporting Policy and Procedure
- Data Protection and Confidentiality Policy
- Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- Confidentiality Audit Policy
- 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.