Bolton Clinical Commissioning Group

Acceptable Use Policy (Including IT, E-mail and Internet)

Policy Number	**IG004**
Target Audience	**CCG**
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	**V5.1**

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
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1.0	August 2013	Exec Team	Approval
1.1	June 2015	IG Team	Reviewed & progress to IM & T Operations Board for approval.
2.0	June 2015	IM & T Operations Board	Approved
3.0	June 2017	IG Team	Reviewed & progress to IM & T Operations Board for approval.
4.0	December 2017	CCG Chief Officer	Approved
4.1	September 2019	IG Team	Reviewed & updated
5.0	October 2019	IG Board	Approved
5.1	**December 2019**	**CCG Chief Officer**	**Approved**

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

Contents

1. Introduction

This policy is to facilitate effective working within NHS Bolton CCG (henceforth referred to as the CCG). The CCG believes it is important to encourage the use of E-mail, internet, and its computer systems for the benefit of the NHS community and wider and therefore allows all employees' access to appropriate information systems and technology.

The purpose of this policy and its associated documents is to outline the acceptable use, practices and responsibilities that are expected when CCG staff are provided with computer, storage, data and media devices (including but not limited to computer, tablet, smartphone) to conduct CCG business which may require interaction with internal networks and business IT systems.

This policy also recognises that the use of portable computing and telephony devices, and access to systems and information from a variety of remote locations is becoming fundamental to the efficient operation of the CCG. This way of working allows information to be made available whilst working on the move, in remote offices, on client sites or from home. Much of the information held by the CCG is confidential data, and / or business sensitive and in some cases may contain personal data and special categories of data, and therefore carries more risk of a breach in security than in a controlled office environment. It is essential that 'mobile' along with office based CCG staff adhere to this policy.

This policy aims to:

- ensure all staff are aware of their responsibilities in the use of the Bolton NHS Foundation Trust and CCGs information systems and CCG information;
- ensure legal and statutory requirements are met; and minimise risk of inadvertent, accidental or deliberate unauthorised access or disclosure of information;
- establish a common set of governance and usage criteria for sending, receiving and storing e-mails that are to be uniformly applied throughout the CCG and its constituent businesses;
- promote awareness of and adherence to the CCG information governance practices;
- provide a foundation for procedures and processes that support the working practices of the organisation.

This policy covers the following areas for acceptable use:

- Responsibilities and use of IT Assets
- Equipment
- Use of Internet and E-mail
- Passphrases / passwords
- Remote use

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. For the remainder of this document staff will be referred to as users.

3. Definitions

Devices
Includes any device that can store images and other information required for the CCG's operational business; i.e. desktop computers. This includes laptops, tablets, personal digital assistants (PDAs), mobile phones / smartphones, as well as digital audio and visual recording / playback devices such as Dictaphones and digital cameras.

Media
Includes any physical items that can store data, images and other information and requires another device to access it i.e. CD, DVD, disc, tape or portable hard drives, USB, memory cards.

Personal Data
Any data which can identify an individual, including but not limited to name, address, telephone number, occupation, date of birth, ethnic group. National Insurance number, NHS number, hospital number or any other information which will allow for the identification of the individual.

Special Categories of Data
Special category data is personal data which is seen as more sensitive (formally sensitive data), and therefore requires more protection. These special categories of data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade Union membership;
- Health Data;
- Sexual life / sexual orientation;
- Genetic data;
- Biometric data.

Business Sensitive Information
Business / commercially sensitive information, including that subject to statutory or regulatory obligations, may be damaging to the CCG or business partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

Information Asset
Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation.

Malware
Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (MALicious softWARE) but as a general term it deals with all forms of viruses, spyware, Trojans and other software designed with malicious intent.

Spam
Mass unsolicited electronic mail received from an un-requested source which attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.

Blogging or Tweeting
This is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video Examples of blogging websites include Twitter.com and Blogging.com.

Social Media
This is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others.

Social Networking
This is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook.com and Linkedin.com

Social Engineering or Blagging
This is the method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets including personal data. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation's staff or maintenance contractor etc.

Intellectual Property Breach
Data / information is a valuable commodity, and much like any other market economy, principles of supply and demand drive it. As risks increase and profits decline, cybercriminals are on the rise. Intellectual Property breach can include unauthorised access, copying or disclosure of a research protected by trade mark, copyrighted materials, and other such information.

Cyber Security
Is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. Becomes more important as more devices are connected to the Internet.

Phishing
Phishing is the attempt to obtain sensitive information such as usernames and passwords, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Virtual Private Network (VPN)
Enables users to send and receive data across a shared or public network as if their computing device where directly connected to the private network.

Shared drive
Sharing a peripheral device (network folder, printer etc.) among several users.

4. Accountability and Responsibilities

Chief Officer
The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

Senior Information Risk Owner
The Senior Information Risk Owner has delegated responsibility for managing the development and implementation of procedural documents to the IT Service Supplier and line managers.

Data Protection Officer
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. The DPO will escalate any data protection acceptable use issues.

Head of IT and the Cyber Security Lead
The Head of IT and the Cyber Security Lead are responsible for ensuring all elements of the CCG's IT infrastructure and connections of the IT's infrastructure comply with this policy.

IT Service
The IT service provider, Bolton NHS Hospitals Foundation Trust, is responsible for the operation of all desktop, laptops and computer peripherals to the codes of practice and operational guides within this policy. They will liaise with the CCG's Head of IT when necessary.

Information Governance Manager
The Information Governance (IG) Manager will provide IG advice and guidance in line with contractual obligations and support CCG management where applicable. In addition the IG Manager will investigate any personal data protection breach arising from acceptable use issues and report and seek guidance from the DPO.

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

Line Managers
Line managers will take responsibility for ensuring that the Acceptable Use Policy is implemented within their department / directorate.

All Staff / Users
All users of the CCG's information and information processing facilities must comply with this policy.

Users are strictly prohibited from using CCG information systems and information in a manner that will:

- break the law and / or have legal implications or liability to the CCG and / or constituent businesses;
- cause damage or disruption to the CCG information systems, including that of its constituent businesses;
- violate any provision set out in this or any other policy, or contravene the CCG Standards of Business Conduct and waste time, decrease productivity or prevent the user from performing their primary responsibilities for the CCG.

Furthermore users will accept:

- that personal use of the CCG'S information systems and equipment is not a right and must be exercised with discretion and moderation;
- the CCG will not accept any liability, in part or whole, for any liability for claims arising out of personal use of the CCG's information systems and equipment or CCG information;
- all data and information relating to the CCG residing on the CCG information systems remains the property of the CCG at all times, unless otherwise stated.

To report any information security breaches via the CCG's incident reporting system, please refer to section 10, Incident Reporting for more information.

5. Equipment

All users will be issued with the appropriate device/s depending on their role.

Users are responsible for their use of devices and connections and must take full responsibility for the security and protections of their devices and any information stored on the device. This includes mobile computing devices including, but not limited to, tablet PCs, laptops, netbooks, smart phones etc. All assigned devices remain the property of the CCG's IT service provider, Bolton NHS Foundation Trust, and must be returned on termination of employment with the CCG or on the instruction of a manager.

Users must ensure that equipment, when used to conduct CCG business, will not be left unsecured at any time. Users are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

Devices required for remote and mobile working are provided to users subject to management approval. Where these are issued, family members or other acquaintances must not be permitted access to the equipment or data. Any device used for remote and mobile working must be connected via a secure network.

It is mandatory for all users to lock their terminals, workstations, laptops, by pressing ctrl/alt/del (or "windows key" and L), iPads and / or Smartphones when not using the device, even for a short period. This will reduce the risk of unauthorised access.

When in the office, mobile equipment should not be left on desks overnight and must be locked securely away. Such devices when being transported should be done so securely and not left in the car overnight, however they may be locked in the boot during the day where there is no suitable alternative.

Where users have been supplied with mobile devices they are responsible for ensuring that it is regularly connected to the CCG network for upgrade of anti-virus software.

Whilst offsite if users decide to use any non-CCG devices for CCG business, under no circumstances must they save personal data, confidential, or commercially sensitive information to these devices. Users are responsible for ensuring that such devices have the relevant security configuration, including up to date anti-virus software

Users must not connect any non-CCG data devices to the CCG network or computers.

Only CCG approved secure data devices or applications must be used for the transfer of personal data, confidential, or commercially sensitive data between computer systems when transfer via the CCG network is not possible. This data must not be transferred onto non-approved devices or networks. Data devices must not be used for data storage.

Users using mobile devices such as laptops are prevented from transferring confidential data as these do not have external device connectors installed.

Users are strictly prohibited from installing software on their CCG or other NHS supplied device.

Authorised users will be permitted to use their personal devices to connect to a CCG network, but will not be permitted to connect to the CCG Corporate domain. In doing so, they must abide by all policies, standards, processes and procedures.

Users must not use the SIM card provided to them with any device other than the one issued with the SIM card without prior approval from the IT department.

If travelling abroad for CCG business, users must notify their line manager and the IT department prior to travel to ensure services will be available and that appropriate tariffs are in place.

Before equipment is returned users must ensure any data is removed. Returned devices will be wiped of any data by IT department.

6. Use of the Internet

The CCG recognises the benefits of the Internet, and electronic communications as valuable business communication tools, which must be used in a responsible, professional and lawful manner. The CCG allows the use of these facilities provided users are protected from any adverse impacts caused by careless or inappropriate usage.

Usage of the CCG Internet is primarily for business use. Occasional and reasonable personal use is permitted, e.g. during breaks, provided that such use does not interfere with performance of duties and does not conflict with CCG policies, procedure and contracts of employment.

The CCG prohibits access to websites deemed inappropriate and monitors access and usage. The monitoring information may be used to support disciplinary action.

Sites deemed inappropriate are those with material that is defamatory, pornographic, sexist, racist, on-line gambling, terrorism and/or such sites whose publication is illegal or risks causing offence.

Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website, the user must immediately inform their line manager or the IT Service Desk.

Financial transactions are not permitted on websites requiring software to be downloaded prior to the transaction being executed. The CCG accepts no responsibility for any charges and/or losses incurred in relation to personal purchases or personal transactions using the CCG information systems regardless of cause. Users are prohibited from having personal items delivered to CCG premises.

The use of the CCG information systems to conduct on-line selling is strictly prohibited.

Only the CCG approved standard and supported Instant Messaging software may be used for business purposes. Users must not circumvent, cause to circumvent, or use tools to circumvent established security and controls applied to any Bolton NHS Foundation Trusts Instant Messaging or other communications software.

Only the CCG approved, standard and supported software for web conferencing and collaborative working must be used. The use of telephony conferencing software

such as Skype and/or Web conferencing such as 'Go To Meetings' is strictly prohibited.

CCG material that is not already in the public domain must not be placed on any mailing list, public news group, or such service. If posting of such materials is necessary, it must be approved by the Communications Department.

Access to file downloads may be restricted as necessary by IT services to ensure network and system security. IT services may also limit access to content to ensure that users comply with the Copyright, Design and Patents Laws, when downloading material from internet sites. The CCG has the right to withdraw internet access from any user and globally ban access to any site without warning.

The CCG recognises that social media is a platform which will allow it to interact with stakeholders in order to enhance its profile, provide information about the role and aims of the organisation, make professional and developmental contacts, and to gauge and understand the views of stakeholders such as patients. The CCG further recognises that social media platforms can benefit users in building and maintaining professional relationships; establishing or accessing professional networks, seeking advice from forums, and accessing resources for professional development. However, users must ensure that confidentiality and the reputation of the business are protected at all times.

Users must be aware that it may be a disciplinary offence to make disparaging remarks about their employer, patients or other employees (even when using their own computer at home) on social networking sites including, but not limited to, Facebook, Twitter or LinkedIn.

Where individuals (staff members) become subject to inappropriate behaviour via social media in connection with their role within the CCG, they should report this immediately following the CCG's Incident Management Procedure, please refer to Section 10. Individuals are advised not to interact until guidance and support have been provided to them. Examples of behaviour deemed unacceptable by Bolton CCG can be found at http://www.boltonccg.nhs.uk/patient-zone/your-feedback-concerns-or-complaints

In summary the use of the internet for the following is strictly forbidden at any time, and anyone using the Internet inappropriately may be disciplined and/or prosecuted:

- Pornography (e.g. accessing child pornography is illegal)
- Illegal or commercial activities (e.g. sites promoting violence, racial discrimination or sexual harassment, sites that are defamatory or that are intended to harass or intimidate other users or using NHS resources to operate a business from work or advertising)
- Activities for financial gain (e.g. lotteries, gambling)
- Downloading material protected by copyright unless express permission has been given (Copyright Designs and Patents Act 1988)

- Hacking (e.g. breaking into other computer systems using the NHSR network as a conduit)
- Fraud (e.g. providing false details or attempting to gain profit illegally
- Social Media misuse

Any user requiring access to a site that has been blocked by the web security software should contact the IT Service Desk in the first instance.

If users have any questions about what is considered to be appropriate or inappropriate use, they are advised to check with their line manager, Head of IT or IT service provider, Bolton NHS Foundation Trust.

7. Use of E-mails

The CCG use NHSMail exclusively to send and receive e-mails. This is managed and offers protection against infected files, mass mailing protection, secured access to logs and quarantined files for audit purposes, generic attachment filtering, e-mail content and attachment inspection, controls to prevent the forwarding of infected e-mails and rules for which attachments can or cannot be sent. This solution states the volume of spam mails and e-mails being filtered.

Like all correspondence, E-mail cannot be regarded as purely private and only seen by the intended recipient. It may also be regarded as official correspondence of the CCG. Remember that E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button.

CCG e-mail accounts must only be used for CCG business, save for the use of CCG e-mail account for personal purposes within reasonable limits which is permitted, provided this does not interfere with the performance of a member of staffs duties. The sending of personal e-mails must be marked accordingly in the subject field.

It is the responsibility of each user to ensure they manage their e-mail appropriately and routinely delete unwanted e-mails or routinely archive e-mails. Users will not be able to send e-mails once their quota has been reached. The burden of responsibility for the appropriate use of e-mail lies with the sender of the message.

The CCG reserves the right to monitor e-mail usages and content.

All e-mails are the property of the CCG, not the user. However, the individual user and the CCG will be held jointly liable for communications containing statements about an individual, group or organisation that are proven to be:

- Defamatory
- Blasphemous
- Sexually or racially offensive
- Breach the duty of confidence

The CCG requires users to be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be on the grounds of sex, race, disability, sexual orientation, age, religion. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by e-mail. Users must not send any messages containing such material. Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal. If any user is subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation they are encouraged to contact their line manager / HR advisor immediately.

Users must not send e-mails containing profanity as it is potentially offensive and these may be blocked by the CCG's IT system.

Users are prohibited from using their e-mail account for personal / business and / or promoting any kind of personal / business activity.

E-mail can be used as documentary evidence in disciplinary proceedings, harassment cases, complaints, libel and legal cases and may be subject to Freedom of Information Act and Subject Access requests

Where possible the sending of personal data via e-mail must be kept to a minimum. Users must check that all personal data is removed from any e-mails or attachments before sending, unless they are permitted to send this type of data. Users are advised to check with their line manager. CCG commercially confidential information must be treated with equal security considerations as personal data.

Users must not send personal data or confidential information to an insecure e-mail address, for example Yahoo, or auto forwarding of e-mails from an NHS mail address to a non NHS mail address.

Secure and encrypted e-mail addresses are nhs.net and a number of secure networks are listed below. NHS Digital has a process that will enable NHSMail users to e-mail safely to non NHSMail accounts (non-accredited or non-secure recipients) including Gmail, Hotmail etc. Users must enter [secure] in the subject line of the e-mail and click send, the e-mail will then be encrypted and protected with a digital signature on the NHSMail platform within the UK. For further information on this process users should liaise with the IG Team.

- .gov.uk*
- .police.uk
- .pnn.police.uk
- .cjsm.net

* Please note the legacy local and central government email domains previously used (gcsx.gov.uk, gsi.gov.uk and gsx.gov.uk) have been switched off and all local and central government organisations should have now migrated to gov.uk email addresses for all email communication as they have adopted the government secure email standard.

Organisations can now achieve the NHS Digital Secure Email Standard, meaning that the security of their email system is a similar standard to NHSmail and emailing to these organisations from NHSmail will be secure. Organisations will retain their email addresses, for example Bolton NHS Foundation Trust continue to use email addresses ending in nhs.uk. Users should use the following link to check whether organisations who advise they have this accreditation appear on the published list: https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#conformance-statements.

Users should refrain from automatically forwarding CCG e-mail to a third party e-mail system, particularly where they contain personal data. Individual messages which are manually forwarded by the user must be checked and not contain personal data or CCG confidential information unless authorised by a line manager.

Users should not initiate the forwarding of chain letters, junk e-mail and / or jokes. If a user receives such an e-mail, the use should immediately report it to their line manager or the IT Service Desk

Users must ensure that they know the e-mail address of the person(s) they are sending a message to and obtain confirmation of receipt of important messages. This is particularly important where messages are sent outside the CCG.

Users must not send e-mails to large number of users unless the recipients have been suitably “Blind Copied” (bcc). This practice will ensure e-mail addresses are not visible to all recipients, which may compromise the confidentiality of one or more recipients.

Users must use care and discretion when drafting e-mails taking care of the confidential nature of the communication.

All e-mails must contain an e-mail signature that conforms to CCG Corporate Guidelines.

Third parties receiving an e-mail may choose to treat it as a formal communication, as legally binding as if it had arrived on CCG headed paper. It is therefore essential that users do not make commitments in an e-mail which exceed their authority or to enter into contracts outside the authority delegated to them by the CCG.

If users receive suspicious e-mails, these must be deleted unless the recipient is able to verify with the sender that the e-mail is genuine.

Under no circumstances must users undertake any further action in relation to suspicious e-mails (such as opening the e-mail clicking on any embedded links, or attachments, or forwarding it on).

Personal e-mail accounts, such as Yahoo, Google and Hotmail should not be used to forward or receive work e-mails.

For further guidance on e-mail use, when and how personal data can be sent, what to do if in receipt of a suspicious e-mail or any further information users are advised to contact the IG Team and the IT Service Desk.

8. Passphrases / Passwords

Each user is allocated an individual identity through a username and password which will be unique to them. All activity performed under that identity becomes accountable. It is therefore vital that users prevent others from misusing their identity by using a strong password.

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.

Users must not allow others to use systems under their identity. Passphrases / Passwords and this includes the use of Smartcards must not be shared. The unauthorised access of passphrases / passwords and / or Smartcards must be reported immediately to the IT Service Desk and an incident must be raised with the Information Governance team in line with the CCG's Incident Reporting Policy/Procedure.

All systems and devices will be password protected to prevent unauthorised use. Passphrases / Passwords must be changed on a regular basis or when prompted to do so.

Users must not add additional passphrases / passwords or security measures to any PC or files without first consulting with IT services.

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 user concerned to contact them and / or the IT Service Desk as soon as possible.

If a user believes, or suspects, that another person is aware of their passphrase / password, this must be changed immediately and IT Services informed. Users must not attempt to remove or bypass the password protection.

Users must not leave any device unattended without activating password protections, (either by logging out, activating a password protected screensaver or locking the device – ctrl+alt+delete).

Users who discover an unattended device and unlocked device, the user discovering the breach must follow the CCG's Incident Management Procedure. If the breach involves personal data, the IG Department must be informed immediately. Any actions undertaken using another user's user identity will be assumed to be those of the account owner.

9. Remote / Mobile Working

Remote and mobile working are both methods which allow users to conduct CCG business whilst being off site. Remote working enables users to access authorised network files and systems via a dedicated VPN connection, whilst mobile working includes any other work off site. Users undertaking remote and / or mobile working will be restricted to the minimum services and functions necessary to carry out their duties.

Use of any information or devices off site must be for authorised work purposes only. Authorisation is to be obtained from the user's line manager following a risk assessment.

Users must ensure that equipment, when used to conduct CCG business, will not be left unsecured at any time. Users are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

If equipment is being used outside of its normal location and might be left unattended, the user is responsible for securing it by other appropriate means.

Only remote access solutions that are provided or agreed with the CCG can be used to access CCG networks when away from CCG workplaces (usually through a dedicated VPN connection). Any device used for remote and mobile working must be connected via a secure network. Please note that if the network is not seen as secure, for example a user may be working in a café or other public building, the VPN connection will not be established. The user maybe able to work offline or even gain limited internet access, users must not access any personal data at this time or business sensitive information.

Users are responsible for ensuring that such devices have the relevant security configuration, including up to date anti-virus software and should ensure they connect to the CCG network on a regular basis to receive these updates.

Users are only permitted to connect non-standard devices to the network via secure method following consultation with IT Services and an approved risk assessment.

All confidential documentation, whether in paper or electronic format must be stored in a secure area when off site, and stored securely during transit.

Whilst offsite if users decide to use any non-CCG devices for CCG business, under no circumstances must they save personal, confidential, or commercially sensitive information to these devices.

All CCG management incidents involving the use of remote working facilities must be reported in accordance with the CCG's Incident Management Procedure. Timely incident reporting is crucial to minimise the risk of data loss. All lost or stolen devices must be reported to the IT Service Desk. Where possible, the IT Service Desk will employ remote wipe technology to remotely disable and delete any data stored when these devices are reported lost or stolen.

10. Incident Reporting

All employees of the CCG including contractors have a duty to report all potential security incidents as soon as possible when they are discovered. The following types of incidents must be reported:

- Any suspected misuse of CCG computer systems, whether accidental or deliberate;
- A system or network security control that is (or is in danger of being) disabled or ineffective;
- A virus or worm infection is suspected on a workstation or server – users must immediately turn the device off;
- Suspecting that personal and / or confidential information is being disclosed or modified without proper authority;
- Suspecting user behaviour which does not comply with this policy or any other information security policies

Users should use the following methods to report an incident:

- User's line manager, by phone, E-mail or in person
- IT Service Desk
- Head of IT
- Incident management system – Safeguard incidents via **https://safeguard.bolton.nhs.uk/index.aspx?sid=%20 or bolccg.incidents@nhs.net.**

Where the incident concerns personal data the IG will be informed and asked to investigate.

For more information refer to the CCG's Data Security & Protection Breaches / Incident Reporting Policy and Procedure.

Dependant on the type of incident the CCG retains the right to:

- Request the monitoring of the use of its information systems for the purpose of protecting its legitimate concerns;
- prohibit personal use of information systems without warning or consultation whether collectively, where evidence points to a risk to the CCG and / or constituent businesses, or individually where evidence suggests a breach of this or any other CCG or NHS Policy may have occurred.

11. Training and Awareness

It is the responsibility of each employee to adhere to the policy.

Users will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods, for example, team meetings; and staff intranet

All users are also mandated to annually complete the Data Security and Protection 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.

12. Monitoring and Review

This policy will be monitored through staff awareness and supporting evidence to the Data Security and Protection 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.

13. 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)
- Common law duty of confidentiality
- Privacy and Electronic Communications (EC Directive) Regulations

In addition, consideration must also be given to:

- Electronic Communications Act 2000
- Other relevant Health and Social Care Acts
- Access to Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008
- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Digital Economy Act 2010 and 2017
- Counter-Terrorism and Security Act 2015

14. Other relevant Procedural Documents

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

- Information Governance Policy
- Corporate Information Security 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

Please note 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.