Bolton Clinical Commissioning Group

Acceptable Use Policy
(Including IT, Email and Internet)

Policy Number	**IG004**
Target Audience	**CCG/CSU Staff**
Approving Committee	**CCG Executive**
Date Approved	**June 2015**
Last Review Date	**June 2015**
Next Review Date	**June 2017**
Policy Author	**Senior IG Officer (CSU)**
Version Number	**V2.0**

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
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

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

Contents

1 Introduction and aims

1.1 This policy is to facilitate effective working within Bolton CCG. The CCG allows all employees' access to appropriate information systems and technology, including the CCG network, and email. However, with this come risks to the CCG. This policy, therefore, sets out the standards applicable for the use of information and information systems within the organisation.

1.2. The aims of this document are to:

- ensure users are aware of their responsibilities in the use of the CCG information systems and information
- ensure legal and statutory requirements are met; and minimise risk of inadvertent, accidental or deliberate unauthorized access or disclosure of information
- establish a common set of governance and usage criteria for sending, receiving and storing emails 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.

1.3 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 Accountability, Responsibilities and Training

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.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

.

2.2 Overall responsibility for the Acceptable Use Policy lies with the Information Security Manager who has delegated responsibility for managing the development and implementation of procedural documents to the IT Service Supplier and line managers.

2.3 The CSU Information Governance Team will provide IG advice and guidance in line with contractual obligations and support CCG management where applicable.

2.4 Line managers will take responsibility for ensuring that the Acceptable Use Policy is implemented within their group or directorate.

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

Staff 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.

2.5 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.

Where relevant, further training and education will be required of staff. Staff will be informed via the Information Governance Training Needs Analysis.

3 Principles

3.1 All data and information residing on the CCG information systems remains the property of the CCG at all times, unless otherwise stated.

3.2 Users accept that personal use of the CCG Information Systems and Equipment is not a right and must be exercised with discretion and moderation. Users further accept the CCG will not accept any liability, in part or whole, for any liability for claims arising out of personal use of the CCG information systems, information and equipment.

3.3 The CCG retains the right to:

- monitor 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.

3.4 Users are not permitted to access, modify, delete or transmit information and/or information systems to which they have not been given explicit access or authorisation.

3.5 Users must follow CCG procedures for password changes and are not permitted to disclose or write down their passwords. The same applies to usernames.

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

3.7 It is mandatory for all users to lock their terminals, workstations, laptops, iPads and/or Smartphones when not using the device, even for a short period.

3.8 Authorised IT Staff and 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.

3.9 Usage of the CCG Internet is primarily for business use. Occasional and reasonable personal use is permitted, e.g. during lunch breaks, provided that such use does not interfere with performance of duties and does not conflict with CCG policies, procedures and contracts of employment. Users are prohibited from using the internet/e-mail facilities for the purpose of advertising, gambling, solicitation of personal goods or services for personal gain or profit, the passing of indecent, subversive or criminal data across or out from the CCG.

3.10 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 constituent businesses,
  - cause damage or disruption to the CCG information systems, including that of its constituent businesses,
  - waste time, decrease productivity or prevent the user from performing their primary responsibilities for the CCG,
- initiating the forwarding of chain letters, junk e-mail and/or jokes. If a user receives such an email, the use should immediately report it to their line manager, the IT Service Desk, or IT Security Manager
- promoting any kind of business, or business activity, except that of the CCG.
- accessing/using personal e-mail accounts, such as Yahoo, Google and Hotmail to forward or receive work e-mails.

3.11 Users must at all times comply with the Copyright, Design and Patents Laws, when downloading material from internet sites.

3.12 Financial transactions are not permitted. 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.

3.13 Only the CCG approved Instant Messaging software may be used for business purposes.

3.14 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.

3.15 Those staff issued with mobile computing devices must ensure that the equipment is secure at all times. Equipment should not be left on desks overnight and must be locked securely away. Such devices should be transported securely, not left in the car overnight, however they may be locked in the boot during the day where there is no suitable alternative.

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

4 Emails

4.1 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.

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

4.3 All e-mails are potentially disclosable to the public under the Freedom of Information Act (FOIA).

4.4 Users must not send personal identifiable data, patient data, sensitive, or confidential information to an insecure e-mail address, for example Yahoo, or auto forwarding of emails from an NHS mail address to a non NHS mail address. Secure e-mail addresses are nhs.net and a number of secure Government networks as listed below. Users should consult their line manager or the IT Security Manager if in doubt.

For clarity: person identifiable, sensitive or confidential information must not be sent unprotected to external non-nhs.net e-mail addresses. For example x.y@CCGA.nhs.uk to x.y@ACUTE.nhs.uk
Non-NHS domains that are secure for the transmission of sensitive data are those with the following suffixes:

- .x.gsi.gov.uk
- .gsi.gov.uk
- .gse.gov.uk
- .gsx.gov.uk
- .police.uk
- .pnn.police.uk
- .cjsm.net
- .scn.gov.uk
- .gcsx.gov.uk>

4.5 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.

4.6 Users must use care and discretion when drafting emails taking care of the confidential nature of the communication.

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

- The Data Protection Act 1998 (including the relevant specific codes of practice e.g. Employment Practices & CCTV)
- Freedom of Information Act 2000 (FOIA)
- The Computer Misuse Act 1990
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Regulation of Investigatory Powers Act 2000

7 Other relevant Procedural Documents

- Corporate Information Security Policy
- Confidentiality and Data Protection Policy
- Secure Transfer of Information Procedure

This list is not exhaustive