North, Central and South Manchester Clinical Commissioning Groups

NHS

Information Governance

IG4 - Acceptable Use Policy

Version: **1.1**

Date Approved: **August 2014**

Document Control Sheet

Title of document:	Acceptable Use Policy		
Supersedes:	Acceptable Use Policy (Version 1.0)		
Placement in Organisation:	Information Governance		
Consultation/Stakeholders	North Manchester CCG Central Manchester CCG South Manchester CCG		
Author(s) name:	Caroline Cross (Information Governance Manager)		
Department/Team:	Information Governance (GMCSU)		
Approved by:	North Manchester Corporate Governance Committee Central Manchester Corporate Governance Committee South Manchester Corporate Governance Committee		
Approval date:	August 2014	Review date:	July 2016
Implementation Date:	October 2014		
Implementation Method:	CCG Website Staff Briefings/Bulletins		
This document is to be read in conjunction with the following documents: *Information Governance Policy*			

Version Control

Version	Date	Brief description of change
V1.0	Oct. 13	CSU IG Team – Approval by CCG Governance Committees
V1.1	Oct. 14	Amendments requested by Governance Committees completed.

PLEASE NOTE: the formally approved copy of this document is held on North, Central and South CCG's website. Printed copies or electronic saved copies must be checked to ensure they match the current online version.

Contents

1.0	Policy Statement
1.1	This policy describes the responsibilities and acceptable use of IT and Information assets within the Clinical Commissioning Group (henceforth referred to as the CCG).
1.2	The CCG reserves the right to amend this policy without notice. If any changes to this policy affect the way employees' use the IT services and information assets, the CCG will provide an avenue for this information to be cascaded down to members of staff and provide reasonable time for the change to be implemented. Employees are responsible for reviewing the policy from time to time for any such changes.
1.3	All staff will be required to read and sign this policy and be appropriately authorised by their manager prior to gaining access to the IT network. All updates to the policy will be communicated to staff by briefings and the Intranet.
2.0	Introduction
2.1	The policy covers the following areas for acceptable use: • Responsibilities and use of IT assets • Use of e-mail and Internet • Network usage.
2.2	Any applications, e.g. Graphnet, NHSmail will also be subject to the NHS terms and conditions of use and their acceptable use policy.
3.0	Aims and Objectives
3.1	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. For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.
4.0	Prohibited Use
4.1	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 staff 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).
4.2	If you have any questions about what is considered to be appropriate or inappropriate use, please check with your manager or IT Security. Known sites falling within the above categories may be blocked by web security software.
4.3	If you require access to a site that is being blocked by the web security software, contact the GMCSU IT Service Desk in the first instance on 0161 765 6684.
5.0	Definitions of Terms Used
5.1	**Information Asset:** Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation.
5.2	**Malware:** Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (**MAL**icious soft**WARE**) but as a general term it deals with all forms of viruses, spyware, Trojans and other software designed with malicious intent.
5.3	**Spam:** Mass unsolicited electronic mail received from an unrequested source which attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.
5.4	**Blogging or Tweeting:** This is using a public website to write an online 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.
5.5	**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.
5.6	**Social Networking:** This is the use of interactive web based sites or social media sites, allowing individuals online interactions that mimic some of the interactions between people with similar interests that occur in life. Popular

	examples include Facebook.com and Linkedin.com.
5.7	**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 a maintenance contractor etc.
5.8	**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 research protected by trade mark, copyrighted materials, and other such information.
6.0	Duties and Responsibilities
6.1	Overall accountability for procedural documents across the organisation lies with the Chief Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.
6.2	Overall responsibility for the Acceptable Use policy lies with the CSU Information Security Manager or equivalent who has delegated responsibility for managing the development and implementation of procedural documents to the IT Service Provider and line managers.
6.3	The GMCSU Information Governance Team will provide IG advice and guidance in line with contractual obligations and support CCG management where applicable.
6.4	Staff will receive instruction and direction regarding the policy from a number of sources: • Policy/strategy and procedure manuals • Line Manager • Specific training courses • Other communication method (e.g. team brief/team meetings); and • Intranet.
6.5	Staff 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.
6.6	The CCG requires all employees 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 or religion. Harassment could include sending sexist or racist

	jokes, making sexual propositions or general abuse by e-mail. You 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 you are subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation you are encouraged to contact your line manager/HR advisor immediately.
7.0	Main Policy
7.1	All data and information residing on the GMCSU information systems remains the property of the CCG at all times, unless otherwise stated. Users accept that personal use of the GMCSU information systems 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 claims arising out of personal use of the GMCSU information systems or CCG information. The CCG retains the right to: • monitor the use of its information systems for the purpose of protecting 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 points to a breach of this or any other CCG or NHS policy. Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not been given explicit access or authorisation. Users are not permitted to share their, or others, usernames or passwords to gain access to any CCG or other information systems. Users must follow established procedures for password changes and are not permitted to disclose or write down their passwords. Users are not permitted to access any information to which they have not been given explicit authorised access. Users are strictly prohibited from installing software on their CCG or other NHS supplied device. 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 should also be locked when not using the device, even for a short period. Authorised staff and IT 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. Illegal downloading, copying and/or storage of copyrighted content onto the CCG information systems is strictly prohibited.

All users must follow Health and Safety guidelines when using information systems.

Users must adhere to Management guidelines, the Information Classification document and information encryption policy when sharing, or sending CCG information internally or externally.

Users are strictly prohibited from using the 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 its constituent businesses.
- violate any provision set out in this or any other policy, or contravene the CCG Code of Conduct/Standards of Business Conduct and waste time, decrease productivity or prevent the user from performing their primary responsibilities for the CCG.

Usage of the GMCSU 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 the performance of duties and does not conflict with CCG policies, procedure and contracts of employment.

Users must, at all times, comply with Copyright, Design and Patent Laws, when downloading material from Internet sites.

The GMCSU 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 GMCSU accepts no responsibility for any charges and/or losses incurred in relation to personal purchases or personal transactions using the GMCSU CCG information systems regardless of cause. Users are prohibited from having personal items delivered to CCG premises.

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

Only the GMCSU approved standard and supported Instant Messaging software may be used for business purposes. Users are prohibited from using

	any other software, not approved by the GMCSU, for Instant Messaging. Users must not circumvent, cause to circumvent, or use tools to circumvent established security and controls applied to any GMCSU Instant Messaging or other communications software. Only the GMCSU approved standard and supported software for web conferencing and collaborative working must be used. Those staff issued with mobile computing devices including, but not limited to, tablet PCs, laptops, netbooks, smart phones etc., must ensure that the equipment is secure at all times. Equipment must not be left on office desks overnight and must be locked away securely. In addition such devices must be transported securely and may only be left in the boot of a car during the day when there is no alternative method of securing the device. Devices must not be left in any vehicle overnight. Users of mobile computing devices will not allow unauthorised access by third parties including, but not limited to, family and friends.
8.0	Review, Monitoring and Compliance
8.1	Users of the Internet must be aware that each site they visit is recorded and logs of sites are regularly examined to ensure inappropriate usage is dealt with. A full security audit trail is maintained of records/sites accessed.
8.2	This policy will be reviewed on at least a two-yearly 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 • organisational changes.
8.3	**Equality Impact Assessment** The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCG legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief. The Equality Impact Assessment has been completed and has identified impact or potential impact as “no impact”.