NHS
Stockport
Clinical Commissioning Group

Acceptable use of IT policy

Version 1

NHS Stockport Clinical Commissioning Group will allow people to access health services that empower them to live healthier, longer and more independent lives.

NHS Stockport Clinical Commissioning Group
7th Floor
Regent House
Heaton Lane
Stockport
SK4 1BS

Tel: 0161 426 9900 **Fax:** 0161 426 5999
Text Relay: 18001 + 0161 426 9900

Website: www.stockportccg.org

Document title :	Policy No:	Version No.
Acceptable use of IT Policy	IG08	1.0

Staff Group covered by this document:
All NHS Stockport CCG employees and contracted staff, any staff on placement (including students, trainees, seconded staff), Governing Body members.
Key Objectives of the document:
To ensure acceptable, safe and secure use of Information Technology and systems To reduce the risk of data loss.
Ratification:
NHS Stockport CCG Information Governance Group
References / Bibliography and Associated Documents:
NHS Stockport CCG - Email Policy NHS Stockport CCG - Information Security Policy NHS Stockport CCG - Remote Access Policy NHS Stockport CCG - Information Governance Assurance Framework NHS Stockport CCG - Procedure for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents (SUIs) NHS Stockport CCG - Safe Haven Guidance GMCSU – Corporate Information Security Policy NHS Mail Acceptable use policy

Signed off by:	Gaynor Mullins
Position:	Chief Operating Office
Date:	10 March 2014 ***A hard copy of this cover page containing a wet signature is held on file by the Head of Compliance.***

Date of issue:	Accountable Director:
10 March 2014	Gary Jones, Chief Finance Officer
Date of Next Review:	**Responsible Committee or Officer:**
March 2015	IG Group (write) Directors meeting (sign-off)

Distribution:
NHS Stockport SharePoint intranet site. *Please note that the SharePoint version of this document is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.*

1. Introduction and aims

1.1. The purpose of this document is to provide guidance to all CCG staff on the acceptable use of CCG information technology and information systems.

1.2. The aims of this document are to ensure:

- Ensure users are aware of their responsibilities in the use the CCG information systems and information
- Ensure CCG legal and statutory requirements are met
- Minimise risk of inadvertent, accidental or deliberate unauthorized access or disclosure of information

2. Scope

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

2.2. For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.

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

3.3. The CCG retains the right to:

- Monitor the use of its information systems for the purpose of protecting its legitimate concerns; and
- Prohibit personal use of information systems without warning or consultation whether collectively, where evidence points to a risk to CCG, or individually where

evidence points to a breach of this or any other CCG policy.

3.4. 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.

3.5. Users are not permitted to share their, or others, usernames or passwords to gain access to any CCG or other NHS information systems and/or information to which they have not been given explicit authorised access.

3.6. Users must follow established procedures for password changes and are not permitted to disclose or write down their passwords.

3.7. Users are strictly prohibited from installing software on their CCG supplied laptop or desktop computer. This must be carried out through the IT Service Desk.

3.8. 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 if for a short period.

3.9. 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.

3.10. Illegal download, copying and/or storage of copyrighted content onto the CCG information systems are strictly prohibited.

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

3.12. Users will adhere to Management guidelines and relevant CCG policies when sharing, or sending CCG information internally or externally.

3.13. 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
- Cause damage or disruption to the CCG information systems
- Violate any provision set out in this or any other policy, or contravene the CCG Code of Conduct/Standards of Business Conduct
- Waste time or decrease productivity or prevent the user from

performing their primary responsibilities for the CCG.

3.14. 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.

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

3.16. 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.

3.17. 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's information systems regardless of cause. Users are prohibited from having personal items delivered to CCG premises.

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

3.19. 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.

3.20. Only the CCG approved, standard and supported Instant Messaging software may be used for business purposes. Users are prohibited from using any other software, not approved by CCG, for Instant Messaging. Users must not circumvent, cause to circumvent, or use tools to circumvent established security and controls applied to any CCG Instant Messaging or other communications software.

3.21. 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 "GoTo Meetings" is strictly prohibited.

3.22. Equipment referred to in 3.19 will not be left on office desks

over night, they must be locked securely away. 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.

3.23. Users of mobile computing devices will not allow unauthorised access by third parties including, but not limited to, family and friends.

4. Accountability, responsibilities and training

4.1. Overall accountability for procedural documents across the organisation lies with the Chief Operating 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.

4.2. Overall responsibility for the Acceptable Use policy lies with the Associate Director of IM&T who has delegated responsibility for managing the development and implementation of procedural documents to the IT Service Provider and line managers.

4.3. The Head of Compliance will also provide advice and guidance to staff in the event of queries relating to this policy.

4.4. Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy, strategy and procedure manuals
- Line manager
- Training courses
- Team briefings and meetings
- SharePoint

5. Monitoring and review

5.1. Performance against Key Performance Indicators will be reviewed on an annual basis and used to inform the development of future procedural documents.

5.2. This policy will be reviewed at least on a 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
- Changes to organisational infrastructure

EQUALITY IMPACT ASSESSMENT – RELEVANCE SCREENING

1.	**Name of the Policy*:**	Acceptable use of IT Policy			
2.	**Person Responsible:**	Paul Fleming			
3.	**What are the main aims of the Policy*?**	To ensure acceptable, safe and secure use of IT systems.			
4.	**Is this a strategic document or a major project?**	**YES**		**NO**	
				✓	
5.a	**What type of impact is this Policy* likely to have on staff or service users from the following equality groups?**	**HIGH**	**MEDIUM**	**LOW**	**DON'T KNOW**
	Age			✓	
	Carers			✓	
	Disability			✓	
	Ethnicity			✓	
	Gender			✓	
	Gender Reassignment			✓	
	Pregnancy & Maternity			✓	
	Religion & Belief			✓	
	Sexual Orientation			✓	
5.b	**Please explain your answer:**	The changes in system and policy have little impact on different equality groups.			

If you have answered YES to question 4, and:

- HIGH impact in 5a - you should move on to a FULL Equality Impact Assessment.
- MEDIUM / LOW / DON'T KNOW in 5a - you should move on to an INITIAL Equality Impact Assessment.

If you have answered NO to question 4, and:

- HIGH / MEDIUM / DON'T KNOW in 5a, you should move on to an INITIAL Equality Impact Assessment.
- LOW impact in 5a, you do not need to complete an Equality Impact Assessment.

6.	**Based on this screening, please indicate if this should proceed to an Initial or Full EIA?**	**INITIAL**	**FULL**	**NONE**
				✓
7.	**Date of EIA Approval:**			

* The term 'Policy' in this context is used to cover any of the following:
Policy / Procedure / Guidelines / Protocol / Service / Practice / Project / or Strategy