Creating a healthier Hull

NHS
Hull Clinical Commissioning Group

Acceptable Computer Use Policy

Name of Policy:	Acceptable Computer Use Policy
Date Issued:	08 March 2016
Date to be reviewed:	March 2018

Policy Title:	Acceptable Computer Use Policy
Supersedes: (Please List)	Acceptable Computer Use Policy
Description of Amendment(s):	Addition of HSCIC Guidance and Caldicott 2 requirements
This policy will impact on:	All Staff
Financial Implications:	No change
Policy Area:	Data Protection
Version No:	1.2
Issued By:	Yorkshire and Humber CSU IG Team
Author:	Yorkshire and Humber CSU IG Team
Impact Assessment Date:	Complete

APPROVAL RECORD		**APPROVAL RECORD**
	Integrated Audit and Governance Committee	08 March 2016
Consultation:	Members of SLT	18 January 2016

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Barry Jackson	First draft for comments	NR	N/A
1.0	Barry Jackson	Approved version	IAGC 11/03/14	11/03/14
1.1	Chris Wallace	Updated to include social media	NR	N/A
1.2	Chris Wallace	Amendments based on feedback	IAGC 08/09/15	

Contents

1 INTRODUCTION AND APPLICABILITY

1.1. This Acceptable Use Policy (AUP) applies to any CCG staff or contractors using NYHCSU IT systems, computer equipment and network services. This includes employed staff, temporary staff and contractors granted access, including access to the guest wireless. It is designed to protect the CCG our employees, customers and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

1.2. The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime. Everyone who works at the CCG is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or the Information Governance Team.

1.3. "Systems" means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

Anyone developing a policy or procedural document is required to complete a Sustainability Impact Assessment. The purpose is to record any positive or negative impacts that the policy is likely to have on each of the CCG's sustainability themes. The Sustainability Impact Assessment form is attached at Appendix 2 of the Policy Framework Guidance Document, together with instructions to help with completion. Include the conclusions in this section of the policy document.

Include the completed assessment paperwork as an Appendix to the policy.

3.3 Bribery Act 2010

The Bribery Act is particularly relevant to this policy. Under the Bribery Act it is a criminal offence to:

- Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and
- Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.

These offences can be committed directly or by and through a third person and other related policies and documentation (as detailed on the CCG intranet) when considering whether to offer or accept gifts and hospitality and/or other incentives.

Anyone with concerns or reasonably held suspicions about potentially fraudulent activity or practice should refer to the Local Anti-Fraud and Corruption Policy and contact the Local Counter Fraud Specialist

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc

5 POLICY PURPOSE & AIMS

5.1 Internet/Intranet Access.

Access is provided to the internet through a secure gateway operated by the CSU IMT. The CSU operates a secure firewall and a range of technical systems to attempt to reduce the risk posed by hackers, criminals and fraudsters who may attempt to attack our systems. Users are advised that the primary purpose for the provision of the internet service is for work related matters. As a secondary use users are permitted to utilise the system for their own personal use subject to compliance with the conditions set out at point 5.2. In addition users are advised that this personal use is classed as a privilege which can be removed and is also subject to monitoring as set out in section 10.

5.2 Social Media

Social media is the social interaction among people in which they create, share or exchange information and ideas in virtual communities and networks. This has taken on many forms in the last 10 years and includes sites such as Facebook and Twitter. The use of social media is increasing within society and has become a common method for people to communicate with each other. Social media offers great opportunities for organisations and individuals to listen and have conversations with people they wish to influence. The NHS has steadily embraced the use of social media to allow them to better engage with service users. Below are some point to be taken into consideration when using social media for both business and personal purposes.

- Employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Be mindful that what you publish will be public for a long time. When online, use the same principles and standards that you would apply

to communicating in other media with people you do not know. If you wouldn‟t say something in an email or formal letter, don‟t say it online.

- Always identify yourself when using social media for work purposes by giving your name and, when relevant, role within the organisation.
- If you are discussing the organisation or organisation related matters in a personal post you should also identify your role within the organisation as above. Write in the first person. You must make it clear that you are speaking for yourself and not on behalf of the organisation.
- If you publish content to any website outside of the organisation that could be perceived to have a connection to the work you do or subjects associated with the organisation, use a disclaimer such as this:
- "My postings on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of the organisation."
- Respect copyright, fair use, data protection, defamation, libel and financial disclosure laws.
- Don't provide the organisation's or another's confidential or other proprietary information on external websites.
- Do not publish or report on conversations that are private or internal to the organisation (for example, do not quote such material in a discussion forum post).
- Respect your audience. Don't use personal insults, obscenities, or engage in any conduct that would not be acceptable in the workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory, such as politics and religion.
- Don't pick fights, be the first to correct your own mistakes, and don't change previous posts without indicating that you have done so.
- If you read something online that you feel is factually incorrect, inaccurate or otherwise needs an official response from the organisation, then you must refer the matter to the Communications Team
- Personal use of social media for should only occur during your own time such as during lunch breaks.
- There are no restrictions on naming the organisation that you work for but it should be considered carefully what is said in regards to your employer.
- If you feel that there is an issue that needs addressing within the organisation then it is advised that you discuss this with your line manager. If this is not appropriate then concerns can be raised through the organisations whistle blowing policy.
- Do not post anything that is libellous or that cannot be supported with evidence. Such actions may be seen as bringing the organisation into disrepute and could lead to disciplinary actions.

5.3 Inappropriate Use

Inappropriate Use of Computer/IT Services. The use of computers and internet services in the following types of activities is specifically prohibited

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with the CCG.
- Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files belonging to others without appropriate authorisation or permission.

- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.
- Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

6 IMPLEMENTATION

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

7 TRAINING & AWARENESS

Staff will be made aware of the policy via team briefing and inductions. This document will be made available on the Intranet.

8 MONITORING & AUDIT

Users are advised that all computer use, including e-mail and internet access is monitored and that staff are advised that in accordance with the Employment Practices Data Protection Code monitoring of Internet use will take place subject to the following guidance:

- Monitoring and IT Security Audit will be carried out by the Information Governance Team.
- All audits carried out will be documented.
- Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment) which could have a legal impact on the CCG.
- Traffic will be monitored as opposed to content unless there are reasons for doing otherwise.
- The Internet History on a local computer is to be set to retain information for 20 days (this is the default setting). Users are not to clear, delete or otherwise change the settings on the History settings on their PC. Such action may lead to further detailed examination of the system being necessary.
- Inappropriate use of the Internet services may result in either facility being withdrawn and may constitute an offence under the CCG disciplinary code.
- Spot checks will be done as opposed to continuous monitoring.

Virus Protection.

IMT will ensure that the appropriate technical steps are taken to reduce the vulnerability of the CCG system to attack from computer viruses. Users are expected to play their part by being aware of the problem of viruses and reporting anything they deem to be suspicious to the IT Helpdesk.

9 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

10 References

Organisational Policies:-

- Information Security Policy
- Data Protection and Confidentiality Policy

Further information on the use of social media can be found below:-

Using Social Media – Practical and Ethical guidance for doctors and medical students – British Medical Association
The Nursing and Midwifery Council's social media guidance.
The Royal College of General Practitioners' social media 'highway code'.
The Royal College of Nursing's 2011 congress discussion about social networking sites (social media).
The General Medical Council's social media guidance.
The Health and Care Professions Council social media guidance (PDF).