

NHS Rotherham Clinical Commissioning Governing Body

Operational Executive – 18th May 2018

Audit and Quality Assurance Committee – 4th September 2018

GP Members Committee (GPMC) – Date

Clinical Commissioning Group Governing Body - 3rd October 2018

Internet Acceptable Use Policy

Lead Executive:	Wendy Allott, Chief Finance Officer
Lead Officer:	Andrew Clayton, Head of Health Informatics
Lead GP:	Dr Richard Cullen, Chair and GP IT Lead

Purpose:
For CCG Governing Body to review the CCG's revised Internet Acceptable Use Policy.
Background:
The Internet Acceptable Use Policy has been reviewed and revised to ensure compliance with the forthcoming General Data Protection Regulation (GDPR) and to introduce the application of the policy to the use of personal devices in the workplace when they are connected to CCG operated networks. The policy was reviewed and accepted by the Information Governance Group in April 2018, prior to amendments to increase the scope to the use of personal devices and subsequently at the and the OE in May 2018.
Analysis of key issues and of risks
There have been no major changes to the content of the policy from the previous version. Changes made to achieve compliance with GDPR (highlighted in yellow) include: <ul style="list-style-type: none">• References to the new General Data Protection Regulation/Data Protection Act 2018• Updated references to old policies (to reflect recent changes)• Cross referenced with Confidentiality Code of Conduct re use of Social Media Changes made to apply the policy to the use of personal devices on the CCG network are highlighted in green.
Patient, Public and Stakeholder Involvement:
N/A
Equality Impact:
Neutral impact
Financial Implications:
N/A
Human Resource Implications:
N/A
Procurement:
N/A
Approval history:
Approved at Information Governance Group in April and the OE in May for escalation to AQuA.
Recommendations:
The Governing Body are requested to endorse the revised Internet Acceptable Use Policy.

Title:	Internet/Intranet Acceptable Use Policy
Reference No:	006-IT
Owner:	Deputy Chief Officer
Author	IG Assurance and Security Manager
First Issued On:	April 2013
Latest Issue Date:	February 2017
Operational Date:	March 2018
Review Date:	March 2020
Consultation Process	
Ratified and approved by:	AQuA XXX 2018 Governing Body XXX 2018
Distribution:	All staff and GP members of the CCG.
Compliance:	Mandatory for all permanent and temporary employees of NHS Rotherham CCG.
Equality & Diversity Statement:	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

Revision History

Date of this revision: May 2018

Revision date	Version No	Previous revision date	Summary of Changes
17/02/10			First Draft
10/03/10			Second Draft Last paragraph in section 2. Removed reference to proxy server in section 4. Added Twitter and Bebo references in section 4. Added copyright statement in section 5. Removed proxy reference in section 6. Added gross misconduct reference in first bullet point of section 8. Added without consent in bullet point 4 of section 8. Added gross misconduct to
09/11/12		10/03/10	Updated to reflect CCG and reviewed.
15/10/14	1.2	09/11/12	Reviewed and updated.
October 2016		15/10/14	Reviewed – no changes required
January 2017	2.0	October 2016	Format change to reflect CCG policy structure
May 2018	2.1	January 2017	Reviewed in line with General Data Protection Regulation – references to GDPR and Data Protection Act 2018 made throughout. Application of the policy extended to personal devices when used on the CCG guest Wi-Fi network.

Contents

Revision History	2
1. Introduction	4
2. Policy Objectives	4
3. Scope	4
4. Users Responsibilities	4
5. Access to the Internet	5
6. Limited Private Use	5
7. Forbidden Use	5
8. Monitoring	6
9. Reporting of Adverse Incidents	6
10. Terms and Conditions for Use of the Internet	6
11. Review and Dissemination	7
12. Associated Documents	7
13. Relevant Legislation	7
APPENDIX A	8

1. Introduction

- 1.1 This Policy governs the use of the Internet and is designed to ensure staff do not breach any NHS policies regarding the use of the Internet facility and also ensure they do not inadvertently put themselves in a position of breaching any other associated guidance or legislation e.g. the General Data Protection Regulation (GDPR), Data Protection Act 2018, the Copyright Designs and Patents Act 1988, the Computer Misuse Act 1990 and the Human Rights Act 1998.
- 1.2 IT Services, including the role responsible for IT Security, are provided to the CCG by The Rotherham NHS Foundation Trust. The IG Assurance and Security Manager at The Rotherham NHS Foundation Trust is the CCG's lead for IT Security.

2. Policy Objectives

- 2.1 This policy has been formulated to ensure:
 - Equity of access to the Internet for those staff who need it
 - Employees know what is and is not acceptable use of the Internet at work
 - Employees are aware that their usage of the internet is subject to monitoring according to published guidelines

3. Scope

- 3.1 This policy must be followed by all users of the CCG's Internet/Intranet including CCG employees, those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students, partner CCGs and eMBED Health Consortium staff working on behalf of the CCG. The policy is applicable to all areas of the organisation and also applies where a personal device is being used that is connected to the CCG's guest Wi-Fi network.

4. Users Responsibilities

- 4.1 All users of the Internet must abide by the conditions detailed within this Policy. Any user found to have breached this Policy may face disciplinary action that could lead to dismissal.
- 4.2 Use of the Internet is permitted and encouraged where such use is suitable for 'business' purposes and supports the objectives of NHS Rotherham CCG.
- 4.3 The Internet is to be used in a manner that is consistent with NHS Rotherham CCG's standards of conduct and as part of the normal role of an employee's job responsibilities.
- 4.4 Any user found to have accessed inappropriate sites (refer to section 5) could be reported to the appropriate authorities and face legal action.
- 4.5 Any person found to have breached this policy may also be investigated by NHS Protect. This may lead to Criminal, Civil and/or disciplinary action against the person.
- 4.6 Staff who use an NHS computer and/or an NHS connection to access the Internet at home or elsewhere must also abide by the conditions detailed within the NHS Rotherham CCG Portable Data Security and Smartphone and Tablet Policy.
- 4.7 Staff must be aware that it may be a disciplinary offence to make disparaging remarks about their patients, other employees and their employer even when using their own computer at home on

social networking sites.

5. Access to the Internet

- 5.1 Full Internet access allows the user to access any area of the Internet. All user activity on the Internet is monitored. The purpose of the Internet is to provide a source of information to assist staff who need it for their job, when they need it. The information available should be accessed primarily for work related purposes, however limited private use is permitted.

6. Limited Private Use

- 6.1 Staff must ensure that they do not spend time on the Internet for personal use in work time. Be aware that internet usage is monitored at all times.
- 6.2 If you do need to use the internet for personal purposes during your work hours (excluding breaks), you must seek the permission of your manager in advance and make up any lost time later that day.
- 6.3 If the privilege of having internet access is abused by staff, they may be asked to account for their access to non-work related web sites, although it is acknowledged that some access to non-work related sites may be necessary at times. Any time spent sending/receiving personal e-mails in work time and on workplace PC's should be made up during the same day.
- 6.4 Internet access is monitored to ensure compliance with business rules and regulations and whilst staff may use the NHS Rotherham CCG Internet connection to connect to social networking sites during their own time such as Facebook and Twitter, they must be aware of the impact this will have on other staff using the internet connection at the same time for legitimate work purposes.
- 6.5 Users must also pay attention to the volume of access. **If the performance of the guest Wi-Fi network is compromised by access for personal use staff may be requested to disconnect their devices.**

7. Forbidden Use

- 7.1 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. sites that may cause embarrassment to others – 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).
- 7.2 If you have any questions about what is considered to be appropriate versus inappropriate use, please check with your manager or the IG Assurance and Security Manager. Known sites falling within the above categories may be blocked by web security software.

If you require access to a site that is being blocked by the web security software, contact the IT

Service Desk in the first instance on 8844.

8. Monitoring

- 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. Information can be shared with the Local Counter Fraud Specialist (LCFS). A full security audit trail is maintained of records/sites accessed.

9. Reporting of Adverse Incidents

- 9.1 In the event of a breach of any of the above conditions, whether deliberate or accidental, the individual discovering such a breach MUST complete and incident report form and report the incident to the Information Governance Lead and/or the IG Assurance and Security Manager.
- 9.2 In the event of a serious breach the Information Governance Lead/ IG Assurance and Security Manager (TRFT) will make the decision as to whether the incident warrants informing the line manager of the individual, the NHS Rotherham CCG Executive with responsibility for IM&T (currently Chief Finance Officer), the Local Counter Fraud Specialist, or if the incident involved patient identifiable information, the Caldicott Guardian.

10. Terms and Conditions for Use of the Internet

- 10.1 The following apply to staff, including agents acting on behalf of NHS Rotherham CCG, and those members of staff who use standalone PCs or personal devices for accessing the Internet. NHS Rotherham CCG has Internet facilities that are available to staff and agents acting on behalf of the organisation to use for business purposes. All users (staff and agents) of these facilities must abide by the conditions detailed below:
- Access is granted only in accordance with this policy. Any member of staff or an agent of NHS Rotherham CCG who may be discovered to be misusing the Internet facilities may be subject to disciplinary action and investigation by NHS Protect which, if proven to be gross misconduct, could result in dismissal.
 - The Internet facilities are provided for approved business use.
 - Any private use of these facilities should be kept to a minimum.
 - In the event of suspected misuse of the Internet facilities, NHS Rotherham CCG reserves the right to monitor, intercept, filter or screen any material accessed that it considers inappropriate without the knowledge or consent of the user.
 - If you are creating or adding to a web based site (such as social media platforms) ensure you avoid the creation or transmission of material that is designed or likely to cause annoyance, inconvenience or needless anxiety, or may infringe the copyright of another person.
 - Users should refer to section '4.2.5 Use of Social Networking Media' in the CCG's Confidentiality Code of Conduct.
 - On no account should NHS Rotherham CCG Internet facilities be used for the accessing and/or transmission of immoral language and/or images.
 - Access for private use is strictly limited and the access of immoral, inappropriate or pornographic images may result in disciplinary action which, if found to constitute gross

misconduct, could lead to dismissal. Additionally, the accessing of pornographic material may result in a criminal offence and NHS Rotherham CCG would seek Police involvement.

- If personal data is to be downloaded from the Internet, for future use on your own database, the IG Assurance and Security Manager or Information Governance Lead for NHS Rotherham CCG must be informed. This is to ensure that the purpose/s for which you wish to use the data are consistent with NHS Rotherham CCG Policy. If the download breaches these requirements, it could be deemed a criminal offence and the organisation could face criminal action and prosecution.
- Penalties for non-compliance may range from withdrawal of access rights to dismissal, for serious breaches of this policy.

11. Review and Dissemination

11.1 This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance. The policy will be reviewed in May 2020.

11.2 This policy will be made available in electronic format and will be located on the CCG Intranet. Any updates are approved by the Audit and Quality Assurance Committee (AQuA) following consideration at the IG Group and are communicated to staff via the intranet and staff briefings.

12. Associated Documents

- Confidentiality Code of Conduct
- Portable Data Security and Smartphone & Tablet Policy
- Safe Haven Policy
- Email policy
- Network Security Policy
- Information Security Policy

13. Relevant Legislation

- General Data Protection Regulation
- Data Protection Act 2018
- Copyright Designs and Patents Act 1988
- Computer Misuse Act 1990
- Human Rights Act 1998

Equality Impact Assessment form 2013

Title of policy or service	Internet Acceptable Use Policy	
Name and role of officers completing the assessment	Andrew Clayton – Head of Health Informatics	
Date assessment started/completed	12.03.18	

1. Outline

Give a brief summary of your policy or service

- Aims
- Objectives
- Links to other policies, including partners, national or regional

This Policy governs the use of the Internet and is designed to ensure staff do not breach any NHS policies regarding the use of the Internet facility and also ensure they do not inadvertently put themselves in a position of breaching any other associated guidance or legislation e.g. the Data Protection Act 1998, the Copyright Designs and Patents Act 1988, the Computer Misuse Act 1990 and the Human Rights Act 1998.

This policy has been formulated to ensure:
Equity of access to the Internet for those staff who need it
Employees know what is and is not acceptable use of the Internet at work
Employees are aware that their usage of the internet is subject to monitoring according to published guidelines

2. Gathering of Information

This is the core of the analysis; what information do you have that indicates the policy or service might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			What actions do you need to take to address these issues?	What difference will this make?
	Positive Impact	Neutral impact	Negative impact		
Human rights		✓			
Age		✓			
Carers		✓			
Disability		✓			
Sex		✓			
Race		✓			
Religion or belief		✓			
Sexual orientation		✓			
Gender reassignment		✓			
Pregnancy and maternity		✓			
Marriage and civil partnership (only eliminating discrimination)		✓			
Other relevant group		✓			

Please provide details on the actions you need to take below.

3. Action plan				
Issues identified	Actions required	How will you measure impact/progress	Timescale	Officer responsible

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	March 2020 – IG Group		
Lead Officer	Andrew Clayton	Review date:	March 2020

Once complete please forward to your Equality lead Elaine Barnes via email elaine.barnes3@nhs.net