NHS

Greater Glasgow and Clyde

INTERNET ACCEPTABLE USE POLICY

Author:	Mike Dench, IT Security Manager
Responsible Director:	Robin Wright, Director of Health Information & Technology
Approved by:	Corporate Management Team
Data approved:	October 2014
Date for Review:	October 2016
Version:	1.5
Replaces previous version:	1.4

Contents

1.0 Introduction

NHS Greater Glasgow and Clyde recognise that access to the Internet is a useful means of communication, a valuable resource and essential to support NHS business.

This policy defines the acceptable use of all Internet connections provided by NHS Greater Glasgow & Clyde. This policy replaces all pre-existing Internet Acceptable Use Policies within NHS Greater Glasgow & Clyde.

This Policy outlines the permissible use of the Internet for NHSGGC when accessing services from the workplace or using NHS resources remotely.

Associated Legislation:

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Copyright, Design and Patents Act 1988
- The Access to Health Records Act 1990
- The RIP Act 2000
- The RIP(S) Act 2000
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Human Rights Act n(2000)
- The Privacy and Electronic Communication (EC Directive) Regulations (2003)

Associated Policies and Standards:

- ISO/IEC 27005:2005
- Caldicott Guardians Manual
- Protecting Patient Confidentiality: NHSScotland Code of Practice
- NHSiS IT Security Manual
- Internet Content Filtering – this document is available in the HI&T Policies section of the Intranet.

2.0 Purpose

The purpose of this Policy is to ensure that the use of computing and network facilities complies with all appropriate legislation and guidance. It also safeguards the reputation of both the organisation and the individual by providing an environment within which staff can safely and securely access external information resources.

NHS Greater Glasgow & Clyde will assist staff in achieving the business aims and objectives of the organisation by providing access to external data resources.

3.0 Scope

This policy applies to all staff employed by NHS Greater Glasgow & Clyde. It also applies to contractors, partnership organisations and visitors not employed by NHS Greater Glasgow & Clyde but engaged to work with, or who have access to the Internet via the NHS Greater Glasgow & Clyde infrastructure.

4.0 Roles and Responsibilities

NHS Greater Glasgow & Clyde will take all reasonable steps to ensure that users of the Internet services are aware of policies, protocols, procedures and legal obligations relating to the use of the Internet. This will be done through training, staff communications and via the intranet.

4.1 Role of Directors and Heads of Departments

Directors and Heads of Departments are responsible for ensuring that staff within their own directorates and departments work in a manner consistent with the principles outlined in the Policy.

4.2 Role of Staff

It is the responsibility of all staff to ensure they have read and understood this Policy and to ensure high standards of confidentiality are met.

Staff must fully understand that all systems and services are provided as business tools and that there is no individual right of privacy when using the Internet.

5.0 Procedures

5.1 Personal Use

Staff are encouraged to use the Internet to access work or education related information. In addition staff should note:

- Reasonable personal use of the Internet is permitted;
- Personal use must not take place during a user’s recorded working hours and only where it does not impact business users;
- Staff have no rights to privacy regarding any use of NHS Greater Glasgow & Clyde computers or networks;
- All Internet access is logged and may be monitored.
- Care should be taken when downloading and forwarding materials or sending links to web pages as the information downloaded or the links forwarded may result in a breach of this or another policy.

5.2 Inappropriate Use

Although the Internet carries vast amounts of useful information, it also carries information, such as pornography and other potentially offensive material, which is inappropriate for staff to access from NHS Greater Glasgow & Clyde computers.

NHS Greater Glasgow & Clyde will prohibit access to any Internet site containing material that is fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, intimidating, racist, pornographic, defamatory or politically motivated. Disciplinary action, or in the worst cases, legal action, may result from improper or deliberate access to such sites;

To minimise the risks of inappropriate material being accessed, technical controls have been added to the network. However, despite the best efforts of the Health Information & Technology Directorate, and users taking reasonable care, users may still stumble over inappropriate material. Should this happen then users are requested to notify the IT Service Desk immediately on 0845 612 5000 (or #650 if in Glasgow area).

5.4 Copyright

Downloading, copying or re-using any third party copyright material from the internet must be in compliance with both the Copyright, Designs and Patents Act 1988, and the NHS Scotland Copy Policy 2011. For more information see the guidance provided on the Copyright page on StaffNet.

5.5 Accuracy

Information obtained through the Internet may not be accurate, and users must check the accuracy, adequacy or completeness of any such information.

5.6 Blocked Websites

NHSGGC must protect its data networks for business purposes and at the same time has a duty of care to its staff to protect them from undesirable material on the internet. For these purposes it has installed filtering software to perform these functions.

Staff should be aware that the filters

- log all internet access
- limit or block access to certain websites for bandwidth, security or legal reasons

Access to certain sites is only permitted via a special option where staff are required to click on a “continue” button as the site may not be of a business nature or may present greater risks. Staff should take additional care when accessing such websites. Categories of websites that require the user to press a “Continue” button include message boards and some religious sites.

Websites that are blocked include those which contain music download and internet radio, and adult content.

Further information is available in the document “Internet Content Filtering”, which is available within the Corporate HI & T Policy section of StaffNet.

5.7 Internet Monitoring

NHS Greater Glasgow & Clyde will monitor employees’ use of the Internet, for the following reasons:

- To ensure that IT network performance meets business needs;
- To ensure that the use of bandwidth for Internet use is appropriate;
- To protect the organisation from Spyware, viruses, and malware;
- To identify any inappropriate and excessive personal use;
- Compliance to this policy;

Internet logs will include a log of all sites visited, by whom and the time spent, along with any downloading activity.

Logs will be scrutinized on a regular basis and any inappropriate activity will be brought to the attention of the appropriate line manager.

6.0 Non-Compliance

NHS Greater Glasgow & Clyde will thoroughly investigate any violations of this policy by means of appropriate management channels.

Any breach of this policy, including excessive personal use of the Internet can result in disciplinary action up to and including dismissal, according to the Board’s disciplinary policy.

All individual employees have a requirement to inform the IT Security Manager immediately should they witness anyone accessing website material categorised broadly as:

- Images of child sexual abuse
- Criminally obscene content
- Incitement to racial hatred content

The IT Security Manager will notify the relevant managers and the police as necessary.

7.0 Personal Use of Social Networking Sites

Access to many 'social networking' websites (e.g. Bebo) and 'streaming media' websites (e.g. Internet Radio) has been blocked. This action has been taken to ensure that the operational IT service provision and business of the organisation is not compromised by the use of these resource intensive websites.

If using Social Media sites from home or from portable computers staff are reminded that they may not to refer to patients, staff members or any events that occur during work time on such sites. Please refer to the Policy on Personal Use of Social Media.

7.1 Corporate Use of Social Media Policy

If you have a legitimate business reason to access these websites, please refer to the Corporate Use of Social Media Policy which can either be accessed from the link or by visiting the H.R. Policy pages on StaffNet.

8.0 Policy Review

This policy will be reviewed on a bi-annual basis, unless the introduction of any new or amended relevant legislation warrants an earlier review.

9.0 Communication & Implementation

This Policy will be communicated through the Information Governance and IT Security Framework.

10.0 Further Advice

For further advice on this Policy please contact the IT Security Manager.

Tel: 0141 347 8137
Email: mike.dench@ggc.scot.nhs.uk

Appendix A

Definitions of Terms Used in the Internet Acceptable Use Policy

The terms of the Email Acceptable Use Policy prohibit certain types of communication. The source of any inappropriate materials could be the Internet and therefore this appendix has been copied from that policy.

1. Defamation & libel

What is defamation & libel?

A published (spoken or written) statement or series or statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

What you must not do

Make or forward statements about people or organisations in any email that you write without verifying their basis in fact. Note that forwarding an email with a slanderous or libellous statement also makes you liable.

What are the consequences of not following this policy?

You and NHS Greater Glasgow & Clyde may be subject to expensive legal action.

2. Harassment

What is harassment?

Harassment is behaviour by one individual, whether intentional or not, that creates feelings of anxiety, humiliation, awkwardness or distress in another which can include verbal or physical threats, offensive jokes, unnecessary bodily contact, offensive language or personal comments about a person’s physical appearance or character.

What you must not do

Use the email system to harass other members of staff by sending or forwarding messages that they consider offensive or threatening.

3. Embarrassing

What is embarrassing?

- Embarrassing emails may cause someone to feel self-conscious or ill at ease or will cause adverse public opinion of NHS Greater Glasgow & Clyde.

What you must not do

- Send or forward emails that contain any potential causes of embarrassment.

What are the consequences of not following this policy?

- NHS Greater Glasgow & Clyde deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be made subject to the Organisation's Disciplinary procedure. Any proven case of harassment will result in disciplinary action against the guilty party which could ultimately lead to their dismissal.

4. Pornography

What is pornography?

- Pornography can take many forms. For example, textual description, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature of email these issues must be taken into consideration. Therefore, NHS Greater Glasgow & Clyde defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. NHS Greater Glasgow & Clyde will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a possible serious disciplinary offence.

What you must not do

- Send or forward emails containing pornography. If you receive an email containing pornography you should report it to your Line Manager.
- Send or forward emails with attachments containing pornography. If you receive an email with an attachment containing pornography you should report it to your Line Manager.
- Save pornographic material that has been transmitted to you.

Note: Within a health setting, there are legitimate reasons for a very small proportion of staff to have access to, or to store images of a sexual nature, therefore this policy will be interpreted with consideration to this requirement.

What are the consequences of not following this policy?

- Users and/or NHS Greater Glasgow & Clyde can be prosecuted or held liable for transmitting pornographic material in the UK and elsewhere.
- The reputation of NHS Greater Glasgow & Clyde will be seriously questioned if pornographic material has been transmitted and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, may be subject to disciplinary action.

Exceptions

- Within certain medical disciplines there are strong business reasons to send and receive sexually explicit materials. Exceptions to this policy apply in these circumstances.