

Use of the Internet Policy

Policy Type:	Information Communication Technology
Directorate Area:	All Directorates
Policy Author/Champion:	Brian A. Parks Policy Author
Contact Details:	Email: brian.parks@rqia.org.uk Telephone number: (028) 90 517522.
Date(s) Equality Screened:	January 2010, August 2014
Date(s) Approved by Executive Team:	22 January 2015
Date of Issue to RQIA Staff:	12 February 2015
Version:	2.0
Date(s) of Review:	August 2014, February 2018
Date(s) of Re-issue to RQIA Staff:	12 February 2015

Contents

Section	Page
1 Introduction	4
2 Scope	4
3 Policy Statement.....	4
4 Responsibilities.....	4
5 Training.....	5
6 Equality	5
7 Connection to the Internet	5
8 Personal Use	5
9 Publishing/Transmitting Information.....	6
9.1 Data Content	6
9.2 Copyright Information	7
10 Use of Internet Services	7
10.1 Use of Internet Based Email Services	7
10.2 Chat Rooms / Forums / User Groups / News Groups.....	8
10.3 Password Management.....	9
10.4 Personal Purchase of Goods or Services.....	9
10.5 Purchase of Business Related Goods or Services	9
10.6 Online Social Networking (OSN) and Blog Sites	9
11.2 Malicious Code	12
12 Registering Email Addresses.....	13
13 Information Verification	13
14 Prohibited Use	13
16 Monitoring.....	15
17 Non-Compliance	15
18 Liability.....	16

Glossary

Abbreviation	Meaning
BSO	Business Services Organisation
HSC	Health and Social Care
ICT	Information Communication Technology
IWF	Internet Watch Foundation
OSN	Online Social Network

1 Introduction

This policy is one of a number of ICT policies. The ICT Delivery Manager is responsible for ICT security within RQIA. However, all RQIA staff members are responsible for the security of the ICT systems through adherence to the ICT security policies.

The purpose of this policy is to outline the permissible use of the internet when accessing services from the workplace or using RQIA resources remotely (e.g. from a laptop connected to RQIA's remote access service).

2 Scope

This policy applies to **all staff** including regular full-time, regular part-time, sessional, board members, contractors, consultants, agency and temporary employees.

This policy is based on the HSC and BSO ICT Security Policies which is regionally enforced across the whole of the HSC. RQIA must adhere to BSO's ICT security policies in order to gain connection to the Health and Social Care (HSC) network and the internet.

Other RQIA policies related to this policy include:

- RQIA ICT Security Policy
- RQIA Use of ICT Equipment Policy
- RQIA Information Security Policy
- RQIA Records Management Policy
- RQIA Flexible Working Policy
- RQIA Flexible Working Scheme Guidance
- RQIA Fraud Policy
- RQIA Style Guide

3 Policy Statement

The main objective of this policy is to provide guidance to RQIA staff on the permissible use of the internet when using RQIA resources.

4 Responsibilities

- 4.1 The **Director of Corporate Services** is responsible for the effective implementation of this policy.
- 4.2 The **ICT Delivery Manager** is responsible for the ICT enablement required by this policy.
- 4.3 All **staff** members have a responsibility to adhere to this policy.

- 4.4 It is the responsibility of **Senior Managers** to ensure that all staff members are aware of and adhere to this policy.

5 Training

On-line training is available to all RQIA staff via The Beeches Management Centre e-learning site.

All ICT Security Policies will be included in staff induction packs.

6 Equality

This Policy was equality screened by the Business Services Organisation (BSO) in January 2010 and was considered to have a low impact implication for equality of opportunity, therefore the Policy does not require to be subjected to a full equality impact assessment.

7 Connection to the Internet

- 7.1 Internet access is not permitted on any networked machine except via RQIA's network.
- 7.2 Direct access through modems (includes broadband services) is not permitted except with the approval of RQIA's ICT Delivery Manager. This will only be granted in exceptional circumstances or for remote access and is subject to the same usage and security policies as RQIA network connections.
- 7.3 Any computer that may previously have been connected to the Internet other than through RQIA's network must not subsequently be attached to the network without first being cleared for connection by the ICT Delivery Manager.

8 Personal Use

- 8.1 Personal use is defined as any use of the internet facilities that does not relate directly to a requirement of the officer's official duties. Thus accessing a site for research purposes, for example, researching advances in cancer care is official use only if such access is necessary as part of the officer's work. Accessing such data for reasons not related directly to a requirement of the officer's work would be classed as personal use of the information.
- 8.2 Any access or use which is **unrelated** to official duties, this may include for example, accessing general news sites, travel information, personal banking, would be classed as personal use.
- 8.3 Personal use of the internet will be permitted, providing that such use:

- complies with the requirements of this document;
- does not compromise the security of official data, result in increased costs or delays or have any negative impact on RQIA's network or on the effective discharge of official business;
- does not result in personal commercial gain.

8.4 Personal use of official internet facilities will be restricted to an individual's own time during non-working hours at lunch breaks and before and after work.

9 Publishing/Transmitting Information

9.1 Data Content

9.1.1 No material of a sensitive/confidential nature may be electronically posted or transmitted unencrypted via the Internet. Material that is considered 'sensitive' and/or confidential may be transmitted via, but not posted on, the Internet provided such material has been encrypted using software approved by the ICT Delivery Manager (i.e. WinZip) and that the intended recipient has been approved according to current relevant approval procedures.

Guidance on encrypting files using WinZip is available in the shared area [Using WinZip](#).

(\\rqia-fap1\RQIA_DATA 08 09\Shared Area\IT_User_Docs\Using_Winzip.doc)

9.1.2 Examples of sensitive and personal information include but are not limited to:

- Copies or extracts of data from clinical systems
- Commercially sensitive information
- Contracts under consideration
- Budgets
- Staff reports
- Appointments – actual or potential not yet announced
- Disciplinary or criminal investigations

9.1.3 Further information on data classification is available from RQIA's Data Security Policy.

9.1.4 The Data Protection Act 1998 regulates what may be done with personal data. It reinforces other legal constraints on the use and disclosure of personal data; for example when data is held under an obligation of confidence, such as medical records. It also outlines a data owners rights to access, alter or remove the personal information which is held by an organisation about them.

9.1.5 Any software licensed to RQIA or must not be uploaded without the express authorisation from the ICT Delivery Manager.

- 9.1.6 Any data owned by RQIA must not be uploaded without the express authorisation from the Head of Information or the Communications Manager.

9.2 Copyright Information

- 9.2.1 RQIA data posted by staff on the Internet must carry one of the following notices or the equivalent RQIA-related phraseology if applicable:

This material is Crown copyright but may be reproduced without formal permission or charge for personal or in-house use.

This material is Crown copyright and all rights are reserved. Applications for permission to reproduce it should be made to RQIA's Information Governance & Records Manager or equivalent.

- 9.2.2 Any document created by staff, irrespective of the intended audience, must include the organisation's name within its title and must clearly identify the author (or appropriate contact) and the date of publication as part of the text.
- 9.2.3 Other documents, or links to other documents, originating elsewhere must be marked with the name of the publishing organisation and the date published (or date posted to the web if date of publication is not known).
- 9.2.4 To establish ownership, and therefore a point of contact, it must be made clear to any readers which documents have been created by the organisation and which have originated elsewhere. Also, while it is often clear from details within the web page of the origin and date of a document, this information is frequently lost when the document itself is printed.

10 Use of Internet Services

10.1 Use of Internet Based Email Services

- 10.1.1 No material of a sensitive/confidential nature may be sent to an internet based email account regardless of whether it is encrypted or not. Examples of internet based email are Gmail and Yahoo!Mail. Examples of sensitive information are listed above.

This is prohibited because

- RQIA have no control over the servers that hold this type of email and therefore cannot restrict access to the mail accounts

- These providers use servers located throughout the world and if the document containing patient/client information is held outside the European Union this could lead to potential breaches of the Data Protection Act (1998)
- The terms and conditions of these services may transfer ownership of the data/documents/pictures to the provider and you do not have the authority to agree to this

10.1.3 Staff are not permitted to access internet based email services using RQIA ICT equipment except where approved by RQIA's ICT Delivery Manager. Refer to the [Website Access Procedure](#) (\RQIA Approved Policies and Procedures\ICT\ICT_Security\Procedures\ICT001_Website_Access_Procedure.pdf)

10.2 Chat Rooms / Forums / User Groups / News Groups

- 10.2.1 Involvement in Chat Rooms / Forums / User Groups / News Groups is permitted only for business purposes and must be authorised by your Senior Manager.
- 10.2.2 When so doing, staff must **not** (unless specifically authorised to do so) speak or write in your organisation's name and must make it clear that their participation is as an individual speaking only for themselves. In any such use of internet facilities, employees must identify themselves, with their own full name, honestly, accurately and completely. The misuse of such facilities may lead to disciplinary action when staff are acting in a personal capacity or even in a business capacity.
- 10.2.3 When participating in a chat room / forum / user group / news group, staff **must**:
- refrain from political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service
 - give due regard to maintaining the clarity, consistency and integrity of RQIA's corporate image and avoid making any inferences that may prove inappropriate from a RQIA perspective

and **must not**:

- reveal sensitively marked information, patient/client data, or any other material covered by RQIA policies and procedures
- use RQIA internet facilities or computing resources to violate applicable laws and regulations in any way or to compromise the security (including confidentiality) of RQIA data

- 10.2.4 RQIA promotes an anti-fraud culture which requires all staff to act with honesty and integrity at all times and to take appropriate steps to safeguard resources. It also provides guidance in reporting suspicions of fraud. Staff should acquaint themselves with RQIA's Fraud Policy before accessing this category of web site.

10.3 Password Management

- 10.3.1 Passwords used by staff for internet accounts must not be duplicated for any other RQIA services or systems.
- 10.3.2 Some service providers, e.g. Microsoft, require a password as part of their registration details. Staff are reminded of the need to protect passwords used within RQIA. Using passwords on the Internet that are similar in content or structure to passwords being used internally may give unnecessary clues to outsiders who may try to break RQIA systems. See the guidance contained in "Management of User Accounts and Passwords" for advice on the structure of passwords.

10.4 Personal Purchase of Goods or Services

- 10.4.1 Staff may use the internet for the occasional purchase of goods and services, e.g. books, flights, CDs, and so on, provided payment is made by the individual and delivery of items purchased is to a **private** address. This **excludes** trading in stocks or commodities.
- 10.4.2 You must **not** create any contractual liability on the part of RQIA. RQIA does not accept any responsibility for the security of credit card details or any other payment method used. Nor does RQIA accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using RQIA systems for personal transactions. All such use is entirely at the individual's own risk.

10.5 Purchase of Business Related Goods or Services

- 10.5.1 The use of the internet for business purchases is permitted provided the same level of authorisation and appropriate use of 'approved' suppliers as dictated by current Procurement and Logistics Service (PALS) purchasing guidelines is applied on each occasion. A copy of the order, and the authorisation, must be kept for records.
- 10.5.2 Particular attention is drawn to those web pages in which there are response forms and/or mail back facilities. For example, some web pages present opportunities to form contracts specifically in relation to purchasing of goods or services.

10.6 Online Social Networking (OSN) and Blog Sites

- 10.6.1 Staff are not permitted to access Social Networking type sites or update their personal blogs using RQIA ICT equipment unless approved for business purposes.

- 10.6.2 Staff should reference RQIA's Fraud Policy before accessing this category of website. RQIA promotes an anti-fraud culture which requires all staff to act with honesty and integrity at all times and to take appropriate steps to safeguard resources. It also provides guidance in reporting suspicions of fraud.
- 10.6.3 If an employee chooses to identify himself or herself as an employee of RQIA on such Internet venues, some readers of such Web sites or blogs may view the employee as a representative or spokesperson of RQIA. In light of this possibility, RQIA requires, that staff observe the following guidelines when referring to RQIA, its activities, other staff members and/or its clients in a blog or on a web site:
- Staff should be respectful in all communications and blogs related to or referencing RQIA, its clients, and/or other staff members;
 - Staff must not use offensive, sexist, racist, hateful or otherwise offensive/discriminatory language;
 - Staff must not use blogs or personal websites to disparage RQIA, its clients, or other staff members;
 - Staff must not use blogs or personal websites to harass, bully, or intimidate other employees or clients. Behaviours that constitute harassment and bullying include, but are not limited to, comments that are derogatory with respect to race, religion, gender, sexual orientation, colour, or disability; sexually suggestive, humiliating, or demeaning comments; and threats to stalk, haze, or physically injure another employee or client;
 - Staff must not use blogs or personal websites to discuss engaging in conduct that is prohibited by RQIA policies, including, but not limited to, the use of illegal drugs, sexual harassment, and bullying;
 - Employees must not post pictures of other employees or clients on a web site without obtaining written permission;
 - RQIA does not host or sponsor a social networking site. The use of any RQIA copyrighted name or logo is not allowed without written permission.
- 10.6.4 Any employee found to be in violation of any portion of this may be subject to disciplinary action.
- 10.6.5 Risks to Consider

All connections to OSN services will pass over the Internet at some point, and connection to the Internet increases the likelihood of

malicious software being unsuspectingly received by the user. This may not only affect the confidentiality, availability or integrity of a user's own machine or data, but could also then be passed on to other users.

OSN users usually share information and opinions in real-time. However, once sent the information is in the public domain and there is no opportunity to recall or fully delete the information. Protectively marked information could be compromised and even unclassified business related information could become more sensitive when aggregated.

Individuals who provide large amounts of personal data to OSN sites may well expose themselves to the threat of identity theft or phishing attacks.

The terms and conditions agreed when signing up to an OSN sites service can often mean that any data posted becomes the property of the OSN site. Some OSN sites (such as LinkedIn) make this data available to others for an additional fee regardless of your privacy settings.

Security measures employed by OSN providers are generally based around users forming 'trust' relationships with other users, where an increase in trust generally results in greater access. Users often form or join common interest groups to socialize further. However, the online world is a virtual world and people can masquerade and therefore not actually be who they pertain to be.

OSN users can often include large attachments and view multimedia content; as a result there may be less bandwidth available for other business requirements.

10.7 Communication Services – Instant Messaging

10.7.1 Use of internet based instant messaging and text / media messaging is prohibited. This includes, but is not limited to AOL Instant Messenger, Yahoo! or MSN.

10.7.2 If there is a business need to access instant or text messaging contact RQIA's ICT Delivery Manager.

11 Downloading of Files and Software

11.1 Appropriate Permission and Licensing

11.1.1 No file (with the exception of documents) should be downloaded from or via the Internet unless doing so is expressly permitted by the ICT Delivery Manager and the terms of the web site.

11.1.2 Particular attention must be paid to any specified licensing requirements or other similar conditions. Staff are **not** permitted to enter into any agreement on behalf of RQIA unless so authorised in writing by the Director of Corporate Services.

Where permission to download is not explicit, to do so could be deemed to be 'hacking' or in breach of copyright laws and expose RQIA to civil and criminal liabilities.

Staff should also avoid downloading large files (> 500 Mb) between 09.00 and 17.00 without first contacting the ICT Delivery Manager to make them aware of your intentions.

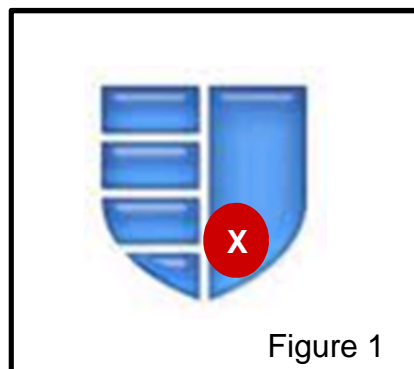
11.2 Malicious Code

11.2.1 Staff must take all steps necessary to avoid the importation of malicious software that may be contained within internet email attachments, downloaded documents or software.

11.2.2 Only officially provided and approved software must be loaded onto computers. This should only be installed by ICT staff, authorised RQIA staff or contracted ICT staff.

11.2.3 Additionally, care should be taken when downloading files:

- check your anti-virus solution is up to date and active. This can be done by checking the blue Sophos shield in the bottom right hand corner of the screen, if Sophos is not up to date there will be a red circle with a white X displayed on the blue shield as shown in Figure 1 below:



If Sophos is not up to date contact the ICT Service Desk immediately;

- only use trusted sites which can be identified as a proper source for the files being downloaded;
- be careful of changes to your own desktop computer. Downloading files might result in changes to its configuration that may not be compatible with the standard setup and render normal services inoperable.

- 11.2.4 If there is any doubt about the integrity of the source or contents of the files to be downloaded staff should in the first instance contact the ICT Delivery Manager.

12 Registering Email Addresses

- 12.1 Staff must only use their RQIA email address to register on websites that are business related. Even then, staff are advised to register only on sites that are trustworthy and have a **privacy policy stating they will not pass on addresses to others**.

13 Information Verification

- 13.1 It is imperative that staff using the Internet understand the importance of verifying any information gathered. While there is much valuable and important knowledge available there is also an equal proportion of information that may be questionable.

14 Prohibited Use

- 14.1 The following list is not exhaustive, but provides an indication of prohibited use:
- Deliberately viewing any pornographic, obscene, indecent or non-clinical sexually explicit material;
 - Deliberately viewing any illegal material;
 - Deliberately viewing any offensive, sexist, racist, hateful or otherwise offensive/discriminatory material;
 - For any commercial activities (e.g. running a business);
 - To perpetrate any form of fraud or criminal activity;
 - The violation of copyright, license agreements or other contracts (e.g. copying and using software for business purposes from a site where there is a clear limitation for personal use only);
 - The download and/or forward of non-business related software or data including music, graphics, videos, text, games, screensavers, wallpapers, entertainment or pirated software;
 - To play internet games or enter on-line competitions;
 - To send offensive or harassing material to others;
 - For personal financial gain (e.g. pay to surf). This includes the use of the classified ads on the HSC Extranet;
 - Bring RQIA or a colleague into disrepute;
 - Any form of defamation;
 - Any form of discrimination;
 - Any form of harassment or bullying;
 - Where it interferes with the work of the individual that is using the internet;
 - Where it interferes with the work of a colleague;

- Where it interferes with the business of RQIA;
 - For illegally distributing any patient or business confidential material;
 - For hacking or gaining access to unauthorised areas;
 - To deliberately waste network resources;
 - To remain continuously connected throughout the day e.g. money markets or sport updates
 - For the deliberate introduction of viruses, spyware or malware;
 - The use of proxy avoidance websites;
 - Streaming video or audio for non-business related use;
 - Any form of internet based instant messaging;
 - Access to streaming media (e.g. You Tube), social networking (e.g. Facebook) and gambling internet websites (e.g. Ladbrokes), except for authorised business purposes;
 - Rich Site Summary (RSS) feeds for personal purposes;
 - For political lobbying;
 - To undertake unauthorised trading at work, whether buying or selling, through internet auction sites such as (but not limited to) e-bay. Trading is defined as any activity, buying or selling, connected with a commercial or business interest.
- 14.2 Inappropriate material may include, but is not limited to, any material of a pornographic, sexist, racist, sectarian, violent or offensive nature; whether in pictures, cartoons, words, sounds or moving images, whether or not purporting to be of a humorous nature. Staff should be aware that the decision as to what material is considered offensive can depend on the perception of the recipient and/or observer, rather than the intention of the sender.
- 14.3 When a site containing inappropriate material is accessed, staff must immediately disconnect from the site, regardless of whether that site had been previously deemed acceptable by any screening or rating program. Such connections must be reported immediately to the ICT Delivery Manager so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation.
- 14.4 Staff should be aware that where attempted access to a website categorised by the Internet Watch Foundation (IWF), e.g. child sexual abuse and criminal matters, is logged RQIA will fully co-operate with the PSNI to identify and take action against any employee.
- 14.5 All individual employees have a requirement to inform the PSNI immediately should they witness anyone accessing website material which may be categorised by the IWF <http://www.iwf.org.uk/> These broadly include:
- Images of child sexual abuse;
 - Criminally obscene content;
 - Incitement to racial hatred content.

15 Blocked Web Sites

- 15.1 A web filtering tool is in place to control access to certain categories of sites and file protocol types.
- 15.2 Only if you have a legitimate business reason to be granted access to one of the blocked sites will a review of it be carried out. This does not guarantee that the restriction will be lifted.
- 15.3 Staff should contact the ICT Delivery Manager, stating the url (internet address) that is blocked (this is displayed on the block page) and the business reason access is required. The procedure for requesting access to a blocked website can be found at the following link [Website Access Procedure](#)
(\RQIA Approved Policies and Procedures\ICT\ICT_Security\Procedures\ICT001_Website_Access_Procedure.pdf)

16 Monitoring

- 16.1 Users of ICT resources, including the internet, should be aware and must accept as a condition of use that their usage of such facilities will be monitored and may be reviewed whether use is for the conduct of official business or for personal use.
- 16.2 Staff should note that, as is permitted by the Employment Practices Code, Part 3 Monitoring at Work ([Employment Practice Code Part 3](#)) (found at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html) RQIA's ICT Delivery Manager will monitor and review internet activity and analyse usage patterns.
- 16.3 The purpose of this monitoring is as follows:
- To monitor and ensure that RQIA's 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;
 - To meet ICT service delivery best practice;
 - To protect the employing organisation from legal liabilities.
- 16.4 RQIA stores the monitoring information securely, with only nominated individuals having access to this information. This information will be held for at least 12 months.

17 Non-Compliance

- 17.1 Any breach of this policy may result in disciplinary action.

- 17.2 Non-compliance can also damage the reputation of RQIA and open RQIA and the individual to a host of legal liabilities some of which would not be covered by the employment contract.
- 17.3 Excessive personal use of the internet may result in the facility being withdrawn.

18 Liability

- 18.1 RQIA does not accept any liability that may arise from employees using the Internet for personal use e.g. personal use of the internet to complete an online transaction, which may at a later stage result in fraud.
- 18.2 Staff should be aware that they might be personally liable to prosecution and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a person that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

For a summary of this policy go to the following link:

[\RQIA Approved Policies and Procedures\ICT\ICT Security\Posters\internetposter.pdf](#)