Northern Ireland Cancer Registry - Information Security and Acceptable Usage Policy

Revisions

Title:	Information Security and Acceptable Usage Policy (NICR-ISMS-AUP)		
Effective Date:	14 Nov 2016	**Version Number:**	1.0
	Name & Position	**Signature**	**Date**
Author:	**Mr Sean McCabe, Quadra Consulting**		
Approved by:	**Dr Anna Gavin Director**		

This is a controlled document and the hard copy may not be the most up to date version. Please ensure you check NICR Sharepoint to ensure you are using the most up to date version.

Revision Log

Previous Version Number	Date of Review/ Modification	Reason for Review/Modification	New Version Number	Next Review By
NA	**Nov 2016**	**First version**	**1.0**	**Nov 17**

Contents

1.0 STATEMENT OF INTENT

This Information Security and Acceptable Use policy sets out what you can and cannot do with the Northern Ireland Cancer Registry (herein called NICR) IT and related equipment. It applies to all NICR/QUB employees, contractors and anyone who uses NICR/QUB systems. In this policy "NICR/QUB Systems" means all NICR or Queens University computers, laptops, notebooks and tablets, smartphones which includes but is not limited to the internet, intranet, and email system.

The purpose of this document is to specify NICR's policy on the acceptable (and prohibited) use of its information and communications technology and sanctions for noncompliance. The policy addresses the need to protect NICR/QUB data, balanced with the need to protect the rights of employee's, board members, contractors, and stakeholders. This policy is a key component of the overarching Information Security Management System.

2.0 SCOPE

2.1 NICR/QUB's ICT facilities and equipment are provided by NICR/QUB's IT department and are made available primarily for the purposes of NICR/QUB's business. The Information Security and Acceptable Use Policy (AUP) is a set of rules that applies to all authorised Users of NICR/QUB's ICT facilities encompassing; employees, board members, contractors, and stakeholders. This policy does not form part of the contract of employment and can therefore be amended without Users' consent.

2.2 ICT facilities encompass (but are not restricted to) the following services provided by NICR/QUB and third parties on its behalf:

- network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers;
- network services, including (but not exclusively) Internet access, web services, email, wireless, messaging, shared filestore, printing, telephony and fax services, CCTV, and physical entry controls;
- NICR/QUB owned (or managed) computing hardware, both fixed and portable, including (but not exclusively) personal computers, laptops, tablets, mobile devices, smartphones, servers, printers, scanners, disc drives (fixed and removable), monitors, keyboards and pointing devices;
- software and databases, including applications and information system, software tools, information services, electronic journals & e-books.

2.3 The ICT facilities available will vary per user group; some users will only be entitled to use some limited facilities.

2.4 All Users are responsible for the success of this Policy and should ensure that they take the time to read and understand it. Before access to NICR/QUB's Systems (including the Internet via NICR/QUB networks) is approved, you are required to read and agree to this Policy. *Please sign page 13 and return to NICR IT department.*

2.5 NICR/QUB may make changes to the Policy at any time. Users will be notified of the changes.

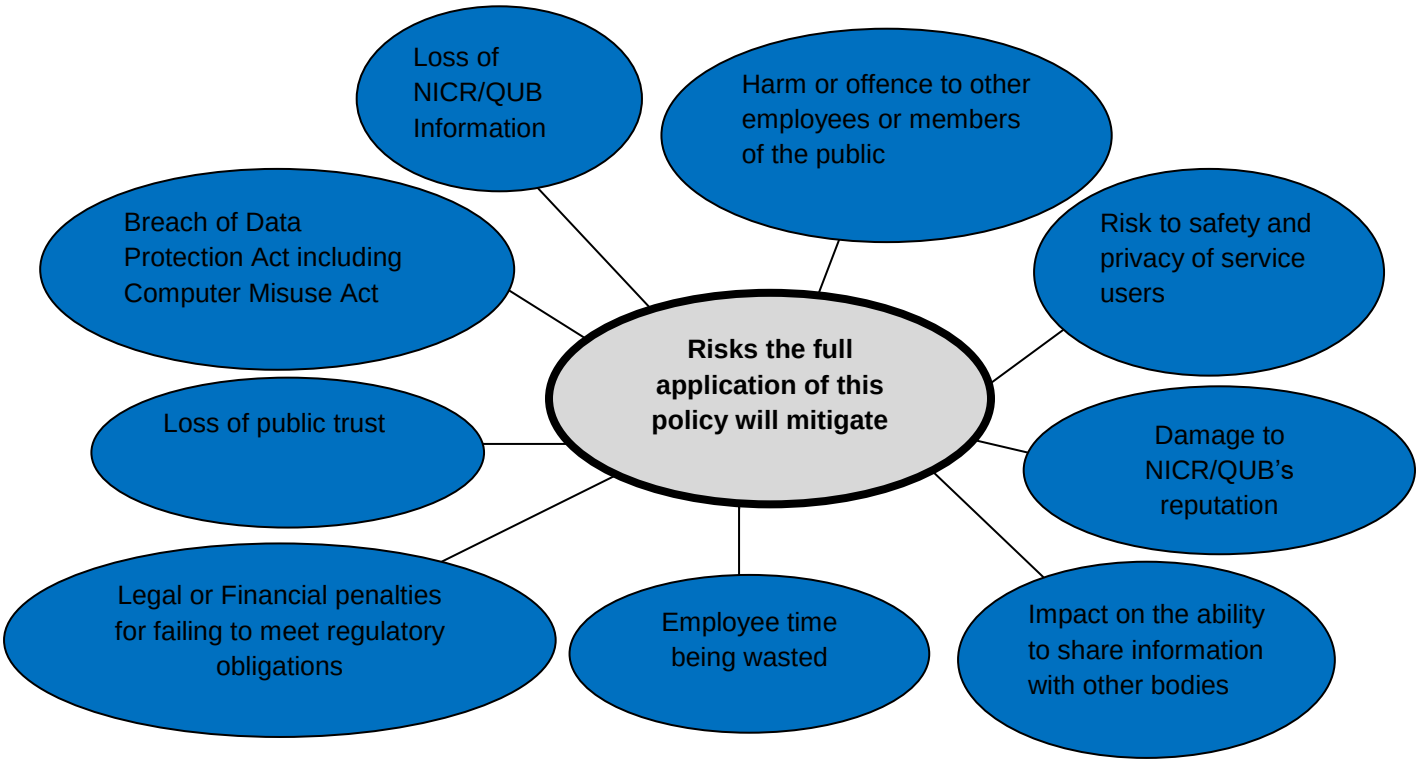
3.0 OBJECTIVES

3.1 Compliance with this procedure will ensure that:

- both individuals and NICR/QUB are better protected from any legal action
- email correspondence with third parties is in an appropriate format and the appropriate levels of confidentiality and security are maintained
- NICR/QUB's IT system perform optimally for their intended use
- NICR/QUB's email system is used in a way that provides a cost effective and efficient form of communication.
- Information gathered, processed and stored by the NICR/QUB is protected always.

4.0 RISKS

4.1 Increased availability of IT systems and internet access bring with it a certain amount of risk to NICR/QUB and employees on a personnel level. Below are the risks this policy is aimed at limiting.



5.0 APPLICABILITY OF POLICY

5.1 NICR/QUB provides its employees with ICT equipment, Internet access and electronic communications services as required for the performance and fulfilment of job

responsibilities. Such IT systems provide many benefits to NICR/QUB and to individual Users. It is NICR/QUB's policy that these facilities like other NICR/QUB assets be used appropriately always. It is vital that you read this policy carefully. If there is anything you do not understand, it is your responsibility to ask your Line Manager to explain or contact the IT Manager. It is essential that you understand that if you fail to comply with this procedure that you may be subject to NICR/QUB's disciplinary procedures and/or legal proceedings. Your failure to comply may result in legal proceedings against NICR/QUB.

6.0 GENERAL PRINCIPLES AND PERSONAL USE

6.1 When you join the organisation, user access will be provisioned based upon your job function, and an account to access systems will be created with an initial password which must be changed the first time you log on or using biometrics depending on the system. Guest users will be allocated a temporary unique set of username and password credentials. Such guest accounts will have appropriately restricted access to NICR/QUB's systems and to external internet services, and will expire automatically after a fixed period.

6.2 Users with elevated credentials are required to change the password for their account in line with the *Credential Management Policy*.

6.3 You are required to change the initial password provided for system access, to a suitable strong password known only to yourself. Selection, use and maintenance of passwords should comply with the terms of NICR/QUB *Credential Management Policy*. Advice on password security is also available from the IT Team in NICR/QUB.

6.4 Once changed by the User, passwords are not accessible or retrievable by any NICR/QUB IT Staff, and restored access to any System should be achieved by reporting such loss or expiry to NICR/QUB's IT Team.

6.5 This Policy provides guidance to you on the standards of behaviour each User is expected to adopt when using systems, what NICR/QUB considers to be inappropriate use of the System and informs you about the monitoring of use of the System.

6.6 All Users are responsible for the success of this Policy and should ensure that they take the time to read and understand it. Before access to the Systems (including the Internet via NICR/QUB/QUB networks) is approved, you are required to read, agree to, and sign this Policy.

6.7 Any misuse or suspected misuse of the system or equipment should be reported to the IT Officer. Failure to comply with the obligations set out in this Policy may constitute a disciplinary offence amounting to gross misconduct and/or termination or suspension of your employment and/or other relationship with NICR/QUB.

6.8 Questions regarding the content or application of this Policy should be directed to the IT Officer or your Line Manager.

6.9 All NICR/QUB facilities must be used in a professional and appropriate manner. Personal use (i.e. non-NICR/QUB business use) of NICR/QUB system by employee Users is allowed so long as such usage:

- does not, as deemed by NICR/QUB, interfere with work, or the working environment of others;
- is not for any illegal activity or any activity which could bring the name of NICR/QUB into disrepute or open NICR/QUB up to legal action;
- does not impact NICR/QUB's ability to provide system access for its legitimate business purposes;
- does not mislead the recipient of communications;
- is not used to support an independent enterprise with which a User is associated without prior approval.

7.0 INFORMATION SYSTEM AND NETWORK SECURITY

7.1. Security of NICR/QUB's system is paramount. Each User must not permit any unauthorised person to gain access to NICR/QUB's System (or to a third party's system) nor seek unauthorised access to a third party's system or documents. NICR/QUB has implemented a number of security controls to safeguard its computer equipment, software and data and these are monitored on a regular basis.

7.2. Unless approved in advance through NICR/QUB's IT Team, under no circumstances must any User:

- introduce or use any program that is not already installed on any System, and/or
- download programs or other executable material from the Internet for use on the system.

7.3. The use of any type of removable media on the system must be approved by the NICR IT Team, and will involve a preliminary check for viruses by an effective scanning utility approved by NICR. NICR provided equipment is normally configured to perform such scans automatically.

8.0 INTERNET USE

8.1. The rules and requirements for e-mail use (see section 11.0 below) apply equally to Internet usage, with the following additional guidelines:

- each User must ensure that, in obtaining information or material from websites or from any other source, the User is not infringing copyright or incurring unauthorised expense to NICR/QUB;
- each User is responsible for ensuring compliance with any terms and conditions governing the use of external websites;
- access to certain sites may be blocked by configurations set through NICR/QUB's IT Team. If any User has a legitimate requirement to be able to access such sites, they should contact the IT Team for authorisation and complete the *Request for Access to a Blocked site* form.
- Users must not visit sites, download material, transfer data or images, store data or images, transmit information or display web pages that may fall into one or more of the following (non-exhaustive) categories (and given the widest meaning of the terms):
  - defamatory, offensive, vulgar or obscene material (including any type of pornography or sexually explicit material);

    - any racist or sexist material;
    - any material that could constitute bullying or harassment (such as on the grounds of sex, including sexual orientation, race or disability);
    - any material that could incite violence or hatred;
    - engaging in any form of intelligence collection from NICR/QUB facilities;
    - engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials;
- any material that could be otherwise considered illegal, or reasonably perceived as falling into one of the above categories;
    - for the conduct of an independent business enterprise or political activity
    - breach of any legal duty owed to a third party such as obligations of confidentiality and contractual duties
    - users must not impersonate any person, or misrepresent their identity or affiliation with others or NICR/QUB
    - users must not give the impression that comments/contributions they make are on behalf of NICR/QUB if this is not the case

8.2. Employee Users must not under any circumstances, even outside normal working hours, at lunchtimes etc., use NICR/QUB's system to participate in any Internet chat room, post messages on any Internet message board or set up or log text regarding NICR/QUB on a blog, where there is a risk that engagement with such media could bring NICR/QUB into disrepute. [The use of social sites, e.g. Twitter, Facebook, etc., may be permitted, but the usage must not interfere with NICR/QUB's work and/or NICR/QUB's legitimate business interests]. Nor should such engagement bring NICR/QUB into disrepute. Please refer to QUB's *Social Media Policy* for guidance.

8.3 Employee Users must not upload information which is confidential or personal in nature to cloud based storage solutions (for example, but not limited to DropBox, OneDrive or Google Drive), without the risk-management consent of their Line Manager. NICR/QUB has concerns about the security of these storage solutions and does not recommend the use of cloud storage solutions to share files over the Internet and encourages individuals to use alternate sources for the sharing/receiving of information. If consent to use a cloud storage solution is given, there will be conditions as to the usage of such a solution.

8.4 Other activities that are strictly prohibited include, but are not limited to:

- accessing NICR/QUB's information using system (or held on the system) that is not within the scope of the User's work;
- misusing, disclosing, or altering employee personal information, (unless regarding alteration ONLY, the user's job description specifically requires them to update the personal data of others);
- deliberate pointing or hyper-linking of NICR/QUB Websites to other internet sites, domain names or IP addresses whose content may be inconsistent with or in violation of the aims or policies of NICR/QUB; and/or
- use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organisation. Users should assume that all materials on the Internet are subject to copyright and/or patented unless specific notices state otherwise.

8.5 Users must not place any NICR/QUB materials (examples: internal documentation, policies, etc.) on any mailing list, public news group, or such service, unless such sharing of materials meets the legitimate business needs of NICR/QUB.

9.0 E-MAIL USE

9.1 The e-mail System is installed as a method of communication for NICR/QUB. If you are an employee whose day to day work normally involves the use of NICR/QUB email, on working days, you should wherever possible ensure you access your e-mails at least once per day; stay in touch by remote access when travelling; use an out of office response when away from the office for more than a day; and endeavour to respond to e-mails marked “high priority” as soon as practicable.

9.2 All e-mail communications may be monitored and subject to random compliance checks at any time as defined below.

9.3 This Policy should not be exploited for personal use. If you are an employee, you should keep personal use to a minimum when within normal working hours, and ensure that such use does not interfere with the proper performance of your duties.

9.4 NICR/QUB’s e-mail System should only be used by employees to conduct NICR/QUB’s business for correspondence that does not infringe this Policy. Wherever possible, employees should use their own personal email accounts held outside of NICR/QUB to conduct correspondence on personal matters that do not relate to their work, or well-being at NICR/QUB.

9.5 Personal and web mail accounts must not be used by employees to conduct NICR/QUB’s business unless the user’s account is inaccessible and the matter to be communicated is urgent. In addition, employees and other Users should not:

- use a NICR/QUB e-mail account to send or receive large/multiple personal attachments including screensavers, games, pictures, executable files, video images and/or presentations from your NICR/QUB or personal e-mail account unless the receipt/sending of such materials relates directly to NICR/QUB's legitimate business activities;
- use a NICR/QUB e-mail account to create, send or receive screensavers, chain letters or notes, junk mail or for-profit messages;
- use another person’s ID to send mail or instant messages unless specifically authorised by that person.
- use a NICR/QUB email account for automated and/or unsolicited bulk emailing. Users with legitimate bulk mailing requirements may request access to a separate bulk mailing facility through NICR/QUB IT Helpdesk

9.6 E-mail encryption facilities are available [for appropriate business use] to ensure the confidentiality and integrity of messages sent between NICR/QUB and its Users and/or third parties. Requests should be directed to the IT Team.

9.7 As with written correspondence, e-mail communications can give rise to binding obligations and expose NICR/QUB to liability in the same way as conventional correspondence.

9.8 Users should not write anything in an electronic communication that could jeopardise the integrity or reputation of NICR/QUB, or which the User cannot or would not be prepared to justify. Always consider whether e-mail is the appropriate medium for a particular message. For example, confidential or sensitive personal information should not be sent within the main text of an e-mail but should be sent in the form of either a password protected file or an encrypted attachment.

9.9 Users must not use the electronic communications system to write, store, send, forward or otherwise transmit any material in any of the following categories, without prior approval of their Line Manager/Director. To do so may constitute gross misconduct and could result in summary dismissal in accordance with NICR/QUB disciplinary policies and procedures. The (non-exhaustive) list of categories includes:

- material which breaches any obligations of confidentiality you have towards NICR/QUB, or NICR/QUB obligations of confidentiality to any third party or is in breach of the proprietary interest, trade mark, trade secret or copyright of others;
- defamatory material;
- abusive, offensive, vulgar, sexually explicit or obscene material (including any type of pornography);
- any material which is untrue or malicious, whether about an employee or someone else outside NICR/QUB;
- information promoting terrorism or cults;
- any material that could constitute bullying or harassment (such as on the grounds of sex, including sexual orientation, race or disability); and/or
- any material that could be otherwise considered illegal, or perceived as falling into one of the above categories.
- material which could breach of any legal duty owed to a third party such as obligations of confidentiality and contractual duties
- material giving the impression that comments/contributions are on behalf of NICR/QUB if this is not the case
- any racist or sexist material;
- any material that could incite violence or hatred

9.10 If a recipient properly asks you to stop sending messages (whether of a personal nature or otherwise), you should always stop immediately.

10.0 VIRUSES

10.1 All e-mails passing through NICR/QUB System are monitored for viruses/malware. However, you should still exercise caution when opening e-mails from unknown external sources or where, for whatever reason, an e-mail appears suspicious (if for example its filename ends in .exe). NICR/QUB's IT team should be immediately informed if a suspected virus is received. NICR/QUB reserves the right to block access to attachments on e-mails to protect the network and to ensure compliance with this Policy. Certain types of attachment are considered high risk, and the range of blocked attachment types is periodically reviewed.

10.2 Users should be wary of incoming emails from an unknown source. Unsolicited emails from unknown sources should be discarded before opening or referred to the

NICR/QUB's IT team. Links from emails should not be followed / used unless the email is from a known reliable sender.

11.0 RETENTION OF E-MAIL MESSAGES

11.1 Every employee should individually create an archive file on a matter-by-matter basis of all important e-mail messages which must be kept for NICR/QUB business, and should ensure its periodic backup. Advice on this is available from NICR/QUB's IT team.

11.2 On a regular basis to conserve space on e-mail servers, QUB may conduct maintenance to review e-mail file storage.

12.0 PRIVACY OF E-MAIL COMMUNICATIONS

12.1 Users should be aware that even if a message is deleted from NICR/QUB's e-mail system, it will still be retained by NICR/QUB either on the daily backups of all data or in other ways. Users should also be aware that e-mail messages may be read by persons other than the intended recipient, including NICR/QUB's employees, or outsiders, under certain circumstances.

12.2 Like hard copy documents, once a User distributes an e-mail message, even if only to an individual recipient, that User (and NICR/QUB) may not be able to control the subsequent distribution, review or retention of that message thereafter.

12.3 Users that receive a wrongly-delivered e-mail should return it to the sender. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

Please note that wherever possible before sending highly confidential information by email, users should consider whether there is a need to encrypt the information and/or use a different means of transfer. *Please refer to guidance document on encryption.*

13.0 IMPROPER MESSAGES PROHIBITED

13.1 Users should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from another User via e-mail should inform NICR/QUB's IT Team or their Line Manager.

13.2 Users should assume that e-mail messages may be read by others and not include anything which would offend or embarrass NICR/QUB, any other reader, or themselves, if it found its way into the public domain.

13.3 In general, Users should not:

- contribute to System congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- sell or advertise using NICR/QUB's communication system or broadcast messages without prior permission from NICR/QUB's IT Team;

- agree to terms, enter in to contractual commitments or make representations by e-mail on behalf of NICR/QUB unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;
- download or e-mail text, music and other content from the Internet subject to copyright protection, unless the owner of such works specifically allows this;
- send messages from another User's computer or under an assumed name unless specifically authorised; or
- as set out below, send highly confidential messages via e-mail or the Internet, or by other means of external communication which are known not to be secure.

14.0 AUTHORITY

14.1 The IT Operator may immediately suspend access to System(s) by any person suspected of contravening any conditions applied to the use of NICR/QUB system. After enquiries, the IT Operator may at their discretion either continue the suspension or reinstate access:

- in the case of employees, after consultation with their line manager,
- in the case of contractors/researchers, after consultation with their line manager/supervisory body.

15.0 MONITORING

15.1 NICR/QUB reserves the right for business reasons and to meet any legal obligations in our role as an employer to monitor, review, record and check the use of all information system, including Internet and e-mail use, from all computers and devices connected to NICR/QUB network(s).

15.2 NICR/QUB may exercise this right to establish facts relevant to NICR/QUB's business and:

- to comply with regulatory practices or procedures;
- to prevent or detect crime;
- to ensure compliance with NICR/QUB policies, including this Policy;
- to investigate or detect unauthorised uses of the System or to ensure the effective operation of the System (e.g. to check if viruses are being transmitted);
- to meet contractual obligations for disclosure of information; and/or
- for business reasons, this may include gathering information about how often information contained on NICR/QUB's IT system is used and by whom to help us develop our strategy and to ensure resources are focused on the correct areas and identify unauthorised usage.

15.3 In these circumstances, individuals do not have a right to privacy when using NICR/QUB managed systems, or in relation to any communication generated, received or stored on NICR/QUB managed systems.

15.4 Access to monitoring applications is strictly controlled. The IT Operator may access all monitoring reports and data if necessary to respond to a security incident.

15.5 NICR/QUB's system enable NICR/QUB's IT employees to monitor and access e-mail communications. For legitimate business reasons, and in order to carry out legal obligations as an employer, use of NICR/QUB's system including the computer system, and any personal use of them, may be continually monitored by NICR/QUB. Monitoring and accessing of e-mail accounts is only carried out to the extent legally required or lawfully permitted or as required as necessary and justifiable for business purposes.

15.6 NICR/QUB reserves the right to monitor e-mails (including personal e-mails), retrieve the contents of and access mailboxes and private directories (and/or check associated Internet use) without further notifying the individual User concerned, where reasonably necessary for the following purposes (this list is not exhaustive):

- where NICR/QUB has a business need to access your mailbox. For example, if an employee User is absent from the office and a Manager has reason to believe that information required for the day's business is in that individual's mailbox. Suitable arrangements need to be made to cover employee absence to avoid such access being required wherever possible;
- to monitor whether the use of the System is legitimate and in accordance with this Policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of suspected or actual wrongful acts; or
- to comply with any legal obligation, such as requests for personal information, litigation or regulatory enquiry or investigations and for NICR/QUB to be able to obtain legal advice and/or to bring or defend legal proceedings.

15.7 E-mail filters have been put in place to monitor e-mail messages for viruses, spam and general compliance with this Policy.

15.8 NICR/QUB reserves the right to monitor Internet and e-mail traffic data (including domain names of websites visited, duration of visits, details of any blocked sites requested, and details of files downloaded from the Internet) at a network level (but covering both personal and business use) in accordance with this Policy. Each User of the System must be aware that the effect of such monitoring or e-mail access may be to reveal certain personal data (including sensitive personal data) about that User as an identifiable individual. For example, a visit to a website relating to a political party or a religious group may indicate your political or religious beliefs.

E-mail monitoring or access for business purposes may also identify the presence of personal e-mails containing sensitive personal data. By accessing websites of this type using NICR/QUB managed IT systems, each User is providing consent to NICR/QUB processing any sensitive personal data that may be revealed by monitoring or access for business purposes as described. Monitoring is carried out automatically and access to any recorded information is limited to a small number of IT employees and then under a strict set of guidelines

15.9 If in doubt and you wish to preserve your personal privacy, do not use NICR/QUB IT system to access any such websites or send/receive personal e-mails.

16.0 LOSSES AND CONFIDENTIALITY / SECURITY BREACHES

16.1 All incidents that constitute a Loss of Hardware or Data, which could potentially lead to a breach of confidentiality, are to be reported to the IT Team. This will instigate investigative procedures to try and establish the nature and threat of the incident.

Incidents could involve;

- Loss of hardware
- Loss of software/data
- Unauthorised access
- Misuse of privileges/system
- Illegal software downloads

17.0 LIABILITY

17.1 Reasonable endeavours are made by NICR/QUB to:

- ensure that the systems are available as scheduled, and function correctly. No liability can be accepted by NICR/QUB for any inability to use our system, any reliance placed on any content displayed on NICR/QUB sites, or any loss of data or delay because of any system malfunction or failure.
- ensure the availability, integrity and confidentiality of information held on the System or in computer media. No liability can be accepted by NICR/QUB because of data being lost or corrupted for any reason or if it is inappropriately accessed.

18.0 CONSEQUENCES OF VIOLATION OF POLICY

18.1 Violations of this Policy will be documented and can lead to revocation of System privileges and/or disciplinary action up to and including termination of employment or legal action.

18.2 Additionally, NICR/QUB may at its discretion seek legal remedies for damages incurred because of any violation. NICR/QUB may also be required by law to report certain illegal activities to the proper enforcement agencies.

19.0 POINTS OF CONTACT

19.1 If you need assistance regarding the following topics related to System usage, you should initially contact NICR/QUB's IT Team for additional assistance.

20.0 USER ACCEPTANCE

I agree to abide by the above 'Information Technology Security and Acceptable Use Policy' and acknowledge that NICR/QUB may enforce it against me if I engage in any illegal activities or in activities that breach or are otherwise unacceptable under this policy. I also acknowledge that NICR/QUB may from time to time monitor e-mail and internet usage to ensure that I am adhering to this policy.

I have retained the copy for future reference:

Name:

Signed: .....

Date: .....

(Return signed to IT Dept)

For IT Dept only

*Date Received:*_____*Signature:*_____

APPENDIX 1

EXAMPLES OF UNACCEPTABLE USE

A. Activities, which are prohibited as potentially illegal include, but are not limited to:

1. Unauthorised copying of copyrighted material including, but not limited to, digitisation and/or distribution of the following works in any form: photographs from any copyrighted source (such as newspapers, magazines or books); musical works and recordings; movies and video; or copyrighted software.
2. Exporting software or technical information in violation of U.K. or other applicable export control laws.
3. Posting or emailing of "make-money-fast" schemes, "pyramid" or "chain" letters or other similar activities
4. Messages of a threatening nature.
5. Making fraudulent offers of products or services.
6. Distributing viruses.
7. Otherwise trafficking in illegal content.
8. Attempting to access the accounts of others, or attempting to penetrate security measures of NICR/QUB or other entities' systems ("hacking"), whether or not the intrusion results in corruption or loss of data.
9. Harassing others by "mail-bombing", "news-bombing" or "unauthorised spamming". "Mail-bombing" constitutes sending more than ten (10) similar mail messages to the same email address. "News bombing" constitutes sending more than 10Mb of data to a newsgroup. "Spamming" constitutes the transmission of unsolicited commercial mass mailings.
10. Sending email messages to more than 10 recipients unless through legitimate directories or address book groups.
11. Sending unsolicited email messages where the recipient objects to the content or receipt of the message is also prohibited under these Terms and Conditions. A message is unsolicited if it is sent to a recipient who has not requested or invited the message. For purposes of this provision, merely making one's email address accessible to the public shall not constitute a request or invitation to receive messages.
12. Utilising, without authorisation, NICR/QUB equipment or any NICR/QUB electronic mail address to send the same or substantially similar unsolicited electronic mail message, whether commercial or not, to a number of recipients other than in the normal course of business. This prohibition extends to the sending of unsolicited mass mailings from another service, which in any way implicates the use of NICR/QUB, its equipment or any of its electronic mail address.

B. Even though not necessarily prohibited by law, you may not use NICR/QUB facilities for or in support of inappropriate purposes, such as:

1. Accessing, storing or transmitting any item or items having indecent, pornographic or violent content.
2. Engaging in activities that are vulgar or profoundly offensive. Profoundly offensive activities include, but are not limited to, posting or transmitting of material discriminating against any groups or persons on the grounds of age, disability, gender, race and ethnicity, religion or belief, sexual orientation and transgender.
3. Revealing your account password to others; or allowing use of your account by others other than authorised users in your workplace
4. Forging any message header, in part or whole, of any electronic transmission, originating or passing through NICR/QUB or QUB services.
5. Installation of automated or manual routines which generate excessive amounts of net traffic, or disrupt newsgroups or email use by others. This prohibition does not apply to use of automatic responses to emails received while away from the office.