Information Systems Security and

Electronic Communications Policy

Document Status Details

Status	Approved by Patrick Freestone
Version History	1.5
Date	7 September 2004
Author	Owain Huw
Reviewed	July 2010, Richard Dormer September 2011, Stephane Vitry

1 Introduction

1.1 Background

Information Systems play a major role in supporting the day-to-day activities of the Centre. The availability, confidentiality and the data integrity of the Centre's systems are essential to the success of its academic and administrative activities. This policy sets out your responsibilities in ensuring the availability and security of the Computing facilities, the maintenance of the Centre's good name and the avoidance of civil or criminal proceedings.

1.2 Scope

This policy relates to all administrative and academic staff, students of the Mary Ward Centre ("the Centre") and all others authorised by the Centre ("the users") and to the use of Centre-owned/leased/rented and on-loan facilities, to all private systems, owned/leased/rented/on-loan, when connected to the Centre network directly or indirectly, to all Centre-owned/licensed data/programs, be they on Centre or on private systems, and to all data/programs provided to Centre by sponsors or external agencies.

1.3 Objectives

The objectives of this policy are:

- To ensure users are aware of their responsibilities when using the Centre's computing facilities, programs, data, network and equipment
- To promote good practice amongst users when using the computing facilities
- Ensure compliance with this Policy Statement and all associated policies
- Promote awareness of, and full compliance with, the relevant UK and European Community (EC) legislation

1.4 Legislation

The Centre has an obligation to abide by all UK legislation and relevant legislation of the EC. The requirement for compliance devolves to all users defined above, who may be held personally responsible for any breach of the legislation. Further details on how the legislation relates to the work of the Centre is available from the IT Department. Of particular importance in the respect of the Centre are:

- Computer Misuse – The Computer Misuse Act (1990)
- Copyright – The Copyright, Designs and Patents Act (1988)
- Data Protection – The Data Protection Act (1998)
- Offensive or defamatory material – The Defamation Act (1996), the Obscene Publications Act (1959), the Protection of Children Act (1978) and the Criminal Justice Act (1988)
- Discrimination – The Sex Discrimination Act 1975, the Race Relations Act (1976) and the Disability Discrimination Act (1995), the Employment Equality (Sexual Orientation) Regulations 2003 and the Employment Equality (Religion or Belief) Regulations 2003

1.5 Sanctions

If a user is in breach of this policy the IT Department may, in consultation with the Vice Principal for Finance and Resources, withdraw or restrict his or her use of computing facilities and user account. Any breach of the regulations may be reported to the Warden to be dealt with under the Centre's disciplinary procedures. Where appropriate, breaches of the law will be reported to the relevant authorities.

2 Use of the Centre's computing facilities

2.1 Introduction

The Centre provides personal computers (PCs) and associated printers and other peripherals for use by its staff and students. While other incidental and occasional personal use may be permitted, such use must not interfere with the employee's work or the student's studies. The person assigned to use an item of equipment will assume responsibility for that equipment. Where appropriate permission from within the normal hierarchy of the Centre has been given, users with temporary access to equipment are expected to behave responsibly in respect of the normal user's data and software on a PC.

2.2 Personal Software

Downloading of any personal software, including freeware and shareware, and its installation from any source onto Centre computing equipment is prohibited without the prior permission from the IT Department. Actions have been taken to prevent the installation of personal software on administration PCs, however members of staff still need to maintain a responsibility over their actions when considering installing any software. Where such permission is granted, and proof of licences have been provided, conditions of use will apply which will be provided in writing at the time of agreement by the IT Department. A regular inventory of software installed on user PCs will be undertaken to ensure compliance, and where software has been installed without prior permission and/or a valid licence, or where the IT Department determines that personal software is interfering with the correct operation of a user's system, the software must be uninstalled from the user's PC. Until this is done, the user's system will not be supported by the IT Department for any purpose; the IT Department may also require the computer system to be disconnected from the Centre's networks. This sub-section applies retrospectively to software installed prior to the introduction of this policy.

2.3 Hardware

The authority to add hardware (other than external devices which have been approved by the IT Department) to a given piece of equipment, to call for engineering assistance, to remove covers, or to approve the action of a user to do any of the above, will rest with the IT Department or Computing Department, who may delegate that authority.

2.4 Storage Media

Magnetic, optical and solid-state media (e.g. hard and floppy disks, CD-ROMs and flash-drives) provided by the Centre for use by staff, remain the property of the Centre at all times. You are responsible for ensuring that your files are stored on network drives, to ensure that they are backed up correctly – data stored on local drives is not backed up. The IT Department is responsible for ensuring the backup of all data and systems on server equipment and other configurable devices.

2.5 Access to resources

All members of staff, including part-time tutors, are allocated an individual username and password. Other than the use of generic usernames for classrooms, you should always use your own username to access computing and network resources – never pretend to be someone else, or allow anyone else to pretend to be you. Always log off when you have finished a session on a computer, and lock your PC when it is unattended. When accessing or displaying confidential information, be careful not to allow others to see it. If someone else needs to read your e-mail or have access to your files, there are other ways to achieve this, which the IT department will advise on.

2.6 Passwords

To log on to any network system, you will be required to enter a password. The disclosure of your password to any other person, other than a member of the IT Department, is expressly forbidden. Similarly, owners of passwords should not write them down. You will be requested to change your password every 3 months. It must conform to the following specification:

- It should not be based on your account name and must not contain a series of letters that make up either a word in a standard dictionary of any language, or represent some name, initials or acronym easily associated with yourself,
- Contain at least eight alphabetic characters,
- Consist of a minimum of 8 characters selected from 3 of the following 4 categories:
  - Uppercase alphabet characters (A-Z)
  - Lowercase alphabet characters (a-z)
  - Numerals (0-9)
  - Non-alphanumeric characters (for example, !$#,%)

3 Privacy

3.1 Introduction

Computing facilities and users accounts are the property of the Centre and are designed to assist in the performance of your work. The Centre respects the right to privacy of its staff in relation to personal material held on its equipment but in order to manage its systems efficiently, authorised systems staff of the Centre will from time to time inspect directories and assess the nature of the content of materials. You should, therefore, have no assumption of absolute privacy, whether it is of a business or personal nature.

3.2 The Right to Monitor

The Centre has the right to monitor any and all aspects of its telephone and computer system that are made available to you and to monitor, intercept and/or record any communications made by employees, including telephones, e-mail or Internet communications. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 you are asked to confirm acceptance when signing this policy in section 6. In addition, the Centre wishes to make you aware that Closed Circuit Television (CCTV) is in operation for the protection of employees and students.

3.3 Absence from work

During periods of absence from work, the Centre may assign equipment to, or allow the use by, another permanent or temporary member of staff. Such staff will be instructed to observe the right to privacy of personal material.

3.4 Termination of employment

Where a person ceases to be a member of staff, they have the right to remove all personal material from Centre systems before departure. They should do this either by electronic transmission or onto magnetic or optical media. All personal mail messages will remain on the server for 6 months, after which time will be permanently deleted. All business-related documents, software, material and media remain the physical and intellectual property of the Centre and may not be removed or copied except where express written permission has been given.

4 Guidelines on the use of the Internet and e-mail

4.1 Introduction

Although e-mail and the World Wide Web provides endless opportunities in the gathering of information and communication with fellow employees, students and other contacts, it also opens up the Centre to new risks and liabilities which are detailed below.

4.2 Personal/private use

Where no cost to the Centre accrues, and where no detriment to the work of the individual or the work of the Centre occurs, reasonable private use of Internet and e-mail services is permitted. The Centre has no interest in monitoring personal use, however the systems in place cannot differentiate and as such, users must appreciate that personal access is possibly subject to audit and monitoring.

4.3 Misuse of services

Excessive private use the Internet and e-mail during working hours, and/or the misuse of the services may lead to disciplinary action and may in certain circumstances be treated by the Centre as gross misconduct. The Centre reserves the right to use the content of access logs and e-mail messages stored on the internal systems, or on archived backups, in any disciplinary process. In addition to the JANET Acceptable Usage Policy (http://www.ja.net) regulating external Internet traffic, the Centre prohibits access to internet resources, or to transmit e-mail messages containing, or referring to resources, which display or offer for sale:

- Any sexually explicit or otherwise obscene or indecent material (whether text or image) relating to any person of any age (whether real or created)
- Any data capable of being resolved into such images or material whether or not such an image is illegal;
- Advice, guidance or assistance on the commission of a criminal offence
- Advocating or encouraging discrimination on the grounds of sex, race, colour, religion, creed, nationality, including hate speech, social status, disability or sexual orientation

5 Communication using Electronic mail (e-mail)

5.1 Managing your e-mail

- Read your e-mail frequently. If necessary, reply as soon as possible, if only to acknowledge receipt of the message. Once you have read and acted on messages in your inbox, you should either delete them or store them in mail folders (please contact the IT Department for further information)
- Regularly delete unnecessary e-mails to prevent over-burdening the system and avoid the use of e-mail attachments when working on collaborative projects where the use of folders on network drives would be more appropriate.
- Make hard copies of e-mail messages which you need to retain for record-keeping purposes.
- During known periods of absence, consider delegating access of your mail system to a colleague or set up an "Out of Office" message to inform correspondents of your unavailability and other avenues of contact.
- Never reply to or forward junk/spam e-mail messages. If you receive a large amount of unsolicited e-mail, contact the IT Department for further advice.
- You may want to obtain e-mail confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system

receiving your message. If in doubt, telephone to confirm receipt of important messages.

5.2 Composing e-mail messages

Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer. E-mails should therefore be drafted with care:

- Do not use e-mail for initiating arguments or inflaming situations or to send what is known as 'flame' mail i.e. to criticise, offend on purpose, or discipline. Such things, if needed, should be done in private and in person.
- Do not make derogatory remarks in e-mails about employees, students, competitors or any other person, as they may constitute libel.
- Consider how the recipient may interpret your e-mail when drafting your message. Avoid using "CAPS", which may be regarded as shouting, or form of words or punctuation that may be misinterpreted.
- Avoid sending trivial or unnecessarily/inappropriately copying or cross-posting ("CC-ing") e-mails.
- Without the use of encryption techniques, e-mail should be regarded as insecure and therefore you should never disclose anything confidential, such as your password or a credit card number.

5.3 Misuse

The following misuse of e-mail will be treated as misconduct and will, in certain circumstances, be treated by the Centre as gross misconduct:

- The transmission of any material reasonably considered to be obscene, abusive, sexist, racist or defamatory or unacceptable as set out in section 4.3. Be aware that such material may also be contained in jokes sent by e-mail.
- Sending bulk e-mail material unrelated to the legitimate educational business of the Centre ("spamming").
- Sending unsolicited e-mail messages requesting other users, at the Centre or elsewhere, to continue forwarding such e-mail messages to others, where those e-mail messages have no educational or informational purpose (chain e-mails).
- Sending e-mail messages which appear to the recipient to come from an someone other than the user sending the message, or using forged addresses ("spoofing").