Policy and Procedures on the Appropriate Student Use of University Electronic Information and Communications Facilities and Services

1 Introduction

1.1 The university employs a diversity of electronic information and telecommunications services.

1.2 There is a range of legal, ethical and other considerations that govern the way in which students use available facilities and services.

1.3 As an example, electronic mail (email) is a useful messaging system, popular because of its speed and informality and because it can be used to send messages/documents to large numbers of people. However, such attributes also make email less private than users may anticipate, eg email intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others.

1.4 This policy:

a) clarifies the applicability of law and of other university policies to the use of University electronic services;

b) specifically supports the generic *Regulations for the Use of Institutional IT, Library and Media Facilities* and

c) defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic information and communications facilities and services.

2 Overview of university provision

2.1 The university encourages students to use the same personal and professional courtesies and considerations in the use of electronic communication services as they would in other forms of communication.

2.2 Although the university makes every effort to prevent unauthorised access, it cannot guarantee that, for example, an email received was in fact sent by the purported sender. As with print documents, in case of doubt, receivers of email messages should check with the purported sender to validate authorship or authenticity.

2.3 Encryption of email is another emerging technology that is not in use in the university as of the date of this policy. This technology enables the encoding of email so that for all practical purposes it cannot be read by anyone who does not possess the right 'key'.

2.4 The answers to questions raised by the growing use of these new technologies are not yet sufficiently understood to warrant their formulation and inclusion in this university policy.

2.5 In due course this policy will be updated to reflect university provision and procedures for users.

3 The purpose of the policy

The purpose of this document is to ensure that:

a) students are informed about the applicability of policies and laws to the use of electronic information and communication services;

b) such services are used in compliance with those policies and laws;

c) students are informed about how concepts of privacy and security apply to such services; and

d) disruptions to university services, and activities dependent on them, are minimised.

4 Scope of the policy

This policy applies to:

a) all electronic information and communication systems and services provided for use by students of, or associated with, Leeds Beckett University – specifically including internet and intranet usage, email, CCTV and telephone services;

b) all users and uses of such student services;

c) all files, images and messages stored on university servers and desktop computers;

d) the content of messages, accessed information and downloaded files; and

e) the associated transactional information such as email headers, subject lines and addresses.

5 Allowable use

The use of any facility or service is limited to university students who have been specifically authorised to have an email account on the student email service.

The Joint Academic Network (JANET) Acceptable Use Policy governs the use of the joint academic network and students should ensure that they are familiar with this policy. (See http://www.ja.net/services/publications/policy/aup.html).

6 Restrictions on use

Facilities and services may not be used for:

a) unlawful activities;
b) commercial purposes not under the auspices of the university;
c) personal financial gain; or
d) any activity which contravenes university regulations.

This specifically covers the creation, display, download, production, store, circulation or transmission of unlawful material, or material that is indecent, offensive, defamatory, racist, threatening, discriminatory or extremist in any form or medium and is strictly forbidden. The university reserves the right to block or monitor access to such material. Where material which could be considered offensive is being accessed, downloaded or transmitted as part of a legitimate academic activity, students must take care to ensure that such legitimacy is established and 'visible'.

7 Code of practice for allowable use

7.1 Representation

When using university facilities and services, students must not give the impression that they are representing the university unless appropriately authorised (explicitly or implicitly) to do so.

7.2 False identity

In using university facilities and services, students must not employ a false identity.

7.3 Interference and disruption

University facilities and services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any such facility or service, or

Unwarranted or unsolicited interference with others' use of these facilities and services.

Examples of non-allowable use include the use of the email service:

a) to send or forward email chain letters;
b) to propagate computer viruses intentionally; and
c) to 'spam', ie to exploit any email or messaging services, or similar broadcast systems, for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email.

7.4 Personal use

The facilities and services may be used for incidental personal use provided that, in addition to the foregoing constraints and conditions, such use does

not incur any significant cost to the university or interfere with the student's academic programme or other obligations to the university.

7.5 Security

Each student is responsible for maintaining the security of their access accreditation (such as usernames and passwords) and must take precautions to prevent unauthorised access. In particular, a password must never be disclosed to another student or other person and each service account must be used only by the student for whom the account was created.

7.6 Monitoring

Section 3(1) of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provides for a system controller's (ie in this case the university's) lawful interception of a communication for the purpose of:

a) monitoring or keeping a record of communications

i) in order to:

aa) establish the existence of facts, or
bb) ascertain compliance with self-regulatory practices or procedures which are applicable either to the system controller in the carrying on of his business; or to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures; or
cc) ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties; or

ii) in the interests of national security, or

iii) for the purpose of preventing or detecting crime; or

iv) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system; or

v) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system (including any [authorised] monitoring or keeping of a record); or

b) monitoring communications for the purpose of determining whether they are communications relevant to the system controller's business;

the university reserves the right to engage in lawful interception of communications as provided for by, and as set out in, Section 7.6 of the Telecommunications Regulations, operating within the framework established by the Regulation of Investigatory Powers Act 2000. The university also reserves the right to block access to websites and other services where necessary, in order to fulfil the University's statutory and regulatory responsibilities.

8 Archiving and retention

The university does not maintain central or distributed archives of student files and messages. Such files and messages held on institutional servers are backed up to ensure system integrity and reliability, not to provide for future retrieval.

Such 'temporary' files as Internet pages stored in the university cache system and email messages deleted by the sender and all recipients will automatically 'drop out of' the backup within a few days. Students should therefore not rely on such devices for purposes of maintaining a lasting record.

9 Service restrictions

The university reserves the right to set quotas on the use of facilities and services including, for example, the storage space occupied by downloaded files or email messages in order to ensure that facilities are used for the full range of designated tasks.

10 Policy violation

10.1 Students who suffer offence or inconvenience as a result of misuse of any electronic facility or service by other students should report the matter to the Help Desk Assistant and/or an Information Desk Assistant within the libraries who will take appropriate action. Please do **not** reply to, or forward, any offensive messages or emails as this just leads to further distribution.

10.2 Violations of the JANET and/or university policies governing the use of such facilities and services, whether reported or identified in some other way, may result in restriction of access to services and other information technology resources. In addition, disciplinary action may be applicable under other university policies and guidelines.

11 Withdrawal of service

Access to the services may be wholly or partially restricted by the university:

a) as a result of a disciplinary process resulting from a violation of this policy; or

b) without prior notice and without the consent of the student when required by, and consistent, with the law.

Such restriction is subject to established university disciplinary regulations and procedures or, in the absence of such procedures or in the case of emergency, to the approval of the Secretary and Registrar or Dean of Innovation North or senior nominee.

12 Responsibility for this policy

The Secretary and Registrar is responsible for the development and maintenance of this policy and procedures document. Any resulting policy changes will be agreed with the Director of IT Services before being issued by the Vice-Chancellor.