Use of information systems policy

1. Introduction

1.1. This policy was previously known as the Use of computers policy.

1.2. This policy defines acceptable and unacceptable use of the university's information systems. The policy applies to any individual who either actively or passively, makes decisions which in turn causes some computation to be performed on DMU systems.

1.3. DMU staff should also refer to the university's **Code of Conduct for DMU Staff** and the **Email, Internet and Social Media Policy**.

2. Scope

2.1. This policy applies to:
- All users of DMU information systems.
- Users of computing resources owned or managed by the university.

2.2. Individuals covered by this policy include (but are not limited to):
- staff
- students
- alumni
- guests
- external individuals and organisations accessing network services via the university's computing facilities.

2.3. Computing resources include all university owned, licensed or managed hardware and software, and the use of the university network via a physical or wireless connection, regardless of ownership of the device connected to the network.

2.4. Unless explicitly stated otherwise in this policy, the '*JANET Acceptable Use Policy'* applies to all users of university computing resources. JANET is defined in section 7.2.

2.5. For the purpose of this policy, reasonable is defined as the level that a reasonably prudent purpose would regard as acceptable in the majority of occasions.

3. Faculty or department policies and regulations

3.1. Faculties/Directorates are permitted to set local rules for the use of computers for which they have responsibility (such as no drinking or eating in computer labs) as long as those rules are not in breach of this or any other university policy.

3.2. Where necessary, Deans of Faculty or Directors may request to implement different policies relating to the use of IT systems for which they have responsibility, subject to agreement with the Information Governance Board.

4. Acceptable use of university IT facilities

4.1. Subject to section 5 and 6 below, DMU information systems may be used for any lawful activity which furthers the aims of DMU and is consistent with the policies of DMU, both at the time of use and in the reasonably foreseeable future after the time of use.

4.2. Student Personal use:

- Subject to section 5 and 6 below, authenticated individuals are allowed to make reasonable use of DMU information systems provided that use does not interfere, or cause any difficulty or distress to others.

4.3. Staff Personal use:

- Subject to section 5 and 6 below, authenticated individuals are allowed to make reasonable use of DMU information systems provided that such use does not interfere with the performance of their duties, or cause any difficulty or distress to others. Such use should be in accordance with the university's **Code of Conduct for DMU Staff** and the **Email, Internet and Social Media Policy.**

4.4. Authentication (user ids and passwords): where a user has been issued with a user id and password, the user is presumed to be responsible for all activity attributable to that identity. To that end:

- If the user has an impairment that prevents them from entering their own username and password, they are permitted to share these details with their nominated support person.
- The user will take all reasonable steps to prevent their personal identity from being used by anyone else.
- Administrative account holders will also take all reasonable steps to prevent the account from being used by anyone else. In particular, passwords must be kept unpredictable to anyone except the legitimate account holder.
- If a user suspects that their password is no longer secret, they should change their password at the first opportunity and notify the ITMS Service Desk (Tel: 0116 2576050 Email: itmsservicedesk@dmu.ac.uk)

5. Inappropriate material

5.1. DMU has a statutory duty to abide by all UK legislation and relevant legislation of the European Community related to the holding and processing of information. Relevant legislation is listed in the Principal Information Security Policy,

5.2. DMU has a general duty, under the Counter Terrorism and Security Act 2015, to have due regard when exercising its functions to the need to prevent people from being drawn into terrorism.

5.3. DMU IT facilities may not be used for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities.

- Create , download, store or transmit material that is:
  - Unlawful
  - Indecent
  - Offensive
  - Defamatory
  - Threatening
  - Discriminatory
  - Extremist
  - Intended to cause annoyance, inconvenience or needless anxiety.
  - Infringes the copyright of another person.
  - Unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the university has chosen to subscribe.

5.4. Further information can be found in the following polices and regulations:
- **Email, Internet and Social Media Policy**
- **Code of Conduct for DMU Staff.**
- **Student Regulations.**

5.5. The university reserves the right to block or monitor access to such material.

6. Inappropriate use

6.1. Negligent, deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
- Wasting university staff effort resources, including time on end systems on any other organisations network, and the effort of staff involved in the support of those systems
- Corrupting or destroying other users' data
- Violating the privacy of other users
- Disrupting the work of other users
- Denying service to other users (for example, by overloading of access links or switching equipment, or any university services or end systems)
- Continuing to use an item of software or hardware after the Director of ITMS or their authorised representative has requested that use cease because it is causing disruption to the correct functioning of the university network
- Deliberate removal or refusal to install any university approved software/application on a university owned device.
- Other misuse of university IT facilities, such as the introduction of "viruses" or other harmful software

6.2. Any attempt to bypass information security safeguards and policies embedded into the university network.

6.3. Deliberate unauthorised access to university services or systems.

6.4. Using "open access" computing facilities (such as computer labs or library computers) for recreational or other non-university work when there are others waiting to use the resource.

6.5. Authenticated sessions: a user must not leave an authenticated (i.e. logged in) session unattended without first invoking a password protected screensaver or similar device.

6.6. This list is not exhaustive and is intended to be illustrative only.

6.7. Further information can be found in the following polices and regulations:
- **Email, Internet and Social Media Policy.**
- **Code of Conduct for DMU Staff.**
- **Student Regulations.**

6.8. The university reserves the right to block or monitor such use.

7. Third Party Regulations

If you use DMU IT facilities to access third party services or resources you are bound by the regulations associated with that service or resource. (The association can be through something as simple as using your institutional username and password).

Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it.

Two examples of this would be:

7.1. **Using Chest agreements**
Eduserv is an organisation that has negotiated many deals for software and online resources on

behalf of the UK higher education community, under the common banner of *Chest agreements*. These agreements have certain restrictions, that may be summarised as: non-academic use is not permitted; copyright must be respected; privileges granted under *Chest agreements* must not be passed on to third parties; and users must accept the User Acknowledgement of Third Party Rights, available at https://www.chest.ac.uk/legal-information/

7.2. **Using Janet, the IT network that connects all UK higher education and research institutions together and to the Internet**
When connecting to any site outside DMU you will be using Janet, and subject to the Janet Acceptable Use Policy, https://community.ja.net/library/acceptable-use-policy the Janet Security Policy, https://community.ja.net/library/janet-policies/security-policy and the Janet Eligibility Policy https://community.ja.net/library/janet-policies/eligibility-policy

The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations you should not infringe the Janet policies.

8. Protecting against unknown or malicious code

The university will put in place appropriate measures to protect against the possible risk of unknown or malicious code infecting devices, these will include:

8.1. Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

8.2. A combination of proactive measures must be used to help manage the risk of malicious code being run on university systems. A combination of the following measures is recommended:

- Deploying antivirus software developed by a reputable supplier, which should be kept fully up to date and used to scan all files: downloaded from the internet, received as attachments to email (or other forms of messaging) and all removable media when inserted.
- Advising computer users to avoid running software or opening files obtained from untrusted sources and to be particularly cautious of accessing files attached to unsolicited email and stored on untrusted media.
- Managing support of computers such that privilege to install software is restricted to experienced computer support staff.

9. Backups

9.1. The university business must not be exposed to unnecessary risk as a result of inadequate data backup arrangements. It is the responsibility of the information owner or custodian for checking or seeking assurance, that the backup arrangements for the facility or service being used are suitable.

9.2. ITMS are responsible for ensuring that backup arrangements published, or agreed with users of the system, are reliably implemented and that users are informed promptly should there be any problems with, or changes to, the backup arrangements.

10. Document approval

Approved by: Chair of the Information Governance Board
Approved Date: 18th December 2018
Review Date: December 2018

Reviewer: Head of Programmes and Planning

11. Document history

11.1. 19th October 2010 – Draft 1 Neil Faver
11.2. 5th October 2012 – Version 1 Neil Faver
11.3. 18th July 2014 Version 2.5 Neil Faver
11.4. 12th January 2016 Version 2.7 Neil Faver
11.5. November 2018 Neil Faver
11.6. December 2018 V2.10 Jon Hill