Use of information systems p olicy

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

2.2. Individuals covered by this policy include (but are not limited to):
- x staff
- x students
- x alumni

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. 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.

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 .

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 c ode

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:
x

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