Computer Acceptable Use Policy

Policy for acceptable use of OU computing systems

An Open University Information Security Common Policy

_Open University – Information Security Team_

Information Classification: **Internal use only**
**Purpose**

This Policy defines the acceptable use of OU computer equipment in order to protect the OU’s information and systems from risks including data loss, viruses and hacking.

**Overview**

The Computer Acceptable Use Policy covers general secure practice for computing devices and should be read in conjunction with the other IT Security Policies.

It is the responsibility of every computer and information user to know and follow this policy.

**Scope**

All users of OU information and information systems with the exception of the use of publicly accessible externally presented OU systems.

**Policy**

1. **Accessing Open University systems**

Users are provided with a user-ID and password to access OU IT services.

1.1 Keep secure and do not disclose your password. Take care to protect your password and or authentication devices where used.

1.2 Passwords must be changed regularly. See the Password Policy for more information.

1.3 All computing devices must be secured with a password with the ‘automatic lock’ feature set to a maximum of 15 minutes.

1.4 Do not allow anyone else to use your user-ID and password.

2. **Ensuring Data Confidentiality**

*See Information Acceptable Use Policy for further details*

2.1 Ensure that your computer is ‘Locked’ whenever you leave it unattended.

2.2 Take extra care with computer equipment and information when working in a public place, for example; protect your password input, if sensitive information is on the screen consider your working location and do not leave your equipment unattended when travelling.
3. **General use and Privacy**

3.1 For security and maintenance purposes, authorised individuals within the Open University central IT teams may monitor all data, systems and network traffic at any time to ensure compliance with this and other security policies and the effective operation of the University’s systems.

3.2 Users of Open University computing systems must abide by all applicable laws.

3.3 The theft or loss of any OU or personally owned IT equipment containing OU data that could be classified as Internal or above must be reported to the IT Helpdesk.

4. **Personal Use**

4.1 At the discretion of your unit, computing resources may be used for personal use so long as it does not cause noticeable or unavoidable cost to the University, interfere with official business or contravene any other Open University policy.

4.2 Subject to personal usage (see 4.1), systems must only be used to fulfil the requirements of your role at the University.

5. **Protection from viruses**

5.1 All computers connected to The Open University’s networks must operate up-to-date antivirus software. Any exception to this must be agreed with the Head of IT Security.

5.2 Files shared, downloaded or received by email may contain viruses. If you are in doubt about a file do not open it and report the issue to the IT Helpdesk.

6. **Enforcement**

6.1 Any breach of these policies is significant as it may undermine the effective running of the Open University and its ability to meet its duties and legal obligations. Failure to comply may lead to disciplinary action, including dismissal for serious or repeated breaches. It may also be the case that your conduct and/or action(s) may be unlawful. The Open University reserves the right to inform the appropriate authorities in such cases. You should note that you may be personally liable for actions and or conduct arising from the use of Open University Systems.