University of Bristol
Information Security Policy

Title: **Acceptable Use**
Reference: **ISP-09**
Status: **Approved**
Version: **1.0.1**
Date: **December 2012**

Contents

- Introduction
- Scope
- User identification and authentication
- Personal use of facilities
- Connecting devices to University networks
- Use of services provided by third parties
- Unattended equipment
- Unacceptable use
- Penalties for misuse

Introduction

This Acceptable Use Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the responsibilities and required behaviour of users of the University's information systems, networks and computers.

Scope

All members of the University (staff, students and associates), members of other institutions who have been granted federated access to use the University's facilities together with any others who may have been granted permission to use the University's information and communication technology facilities by the Director of IT Services are subject to this policy.

User identification and authentication

Each member will be assigned a unique identifier (userID) for his or her individual use. This userID may not be used by anyone other than the individual user to whom it has been issued. Each member will be assigned an associated account password which must not be divulged to anyone, including IT Services staff, for any reason. This University password should not be used as the password for any other service. Individual members are expected to remember their password and to change it if there is any suspicion that it may have been compromised.

Each member will also be assigned a unique email address for his or her individual use and some members may also be given authorisation to use one or more generic (role based) email addresses. Members must not use the University email address assigned to anyone else without their explicit permission.

Email addresses are University owned assets and any use of these email addresses is subject to University policies.

Personal use of facilities

University information and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the University. Very occasional personal use is permitted but only so long as:

- it does not interfere with the member of staff's work nor the student's study
- it does not contravene any University policies
- it is not excessive in its use of resources

University facilities should not be used for the storage of data unrelated to membership of the University. In particular, University facilities should not be used to store copies of personal photographs, music collections or personal emails.

Members of staff and research postgraduates should not use a personal (non-University provided) email account to conduct University business and should maintain a separate, personal email account for personal email correspondence.

All use of University information and communication facilities, including any personal use is subject to University policies, including the Investigation of Computer Use Policy (ISP-18).

Connecting devices to University networks

In order to reduce risks of malware infection and propagation, risks of network disruption and to ensure compliance with the JANET Acceptable Use and Security policies, it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the University's wireless networks.

To further reduce risk of data loss, members of staff and research postgraduates should not connect any personally owned peripheral device which is capable of

storing data (for example, a personally owned USB stick) to any University owned equipment, irrespective of where the equipment is located. Only University owned peripheral devices may be connected to University owned equipment.

Any device connected to a University network must be managed effectively. Devices which are not are liable to physical or logical disconnection from the network without notice.

Use of services provided by third parties

Wherever possible, members should only use services provided or endorsed by the University for conducting University business. The University recognises, however, that there are occasions when it is unable to meet the legitimate requirements of its members and that in these circumstances it may be permissible to use services provided by other third parties.

Further information is available in the Information Handling Policy (ISP-07) and the Outsourcing and Third Party Compliance Policy (ISP-04).

Unattended equipment

Computers and other equipment used to access University facilities must not be left unattended and unlocked if logged in. Members must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended.

Particular care should be taken to ensure the physical security of University supplied equipment when in transit.

Unacceptable use

In addition to what has already been written above, the following are also considered to be unacceptable uses of University facilities. These restrictions are consistent with the JANET acceptable use policy (by which the University is bound) and the law.

- Any illegal activity or activity which breaches any University policy (see the Compliance Policy - ISP-03).
- Any attempt to undermine the security of the University's facilities. (For the avoidance of doubt, this includes undertaking any unauthorised penetration testing or vulnerability scanning of any University systems.)
- Providing access to facilities or information to those who are not entitled to access.

- Any irresponsible or reckless handling of University data (see the Information Handling Policy - ISP-07).
- Any use which brings the University into disrepute.
- Any use of University facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business of the University.
- Creating, storing or transmitting any material which infringes copyright.
- Creating, storing or transmitting defamatory or obscene material. (In the unlikely event that there is a genuine academic need to access obscene material, the University must be made aware of this in advance and prior permission to access must be obtained from the Director of IT Services.)
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of the University's facilities.
- Failing to report any breach, or suspected breach of information security to IT Services.
- Failing to comply with a request from an authorised person for you to change your password.

Penalties for misuse

Minor breaches of policy will be dealt with by IT Services. Heads of Department may be informed of the fact that a breach of policy has taken place.

More serious breaches of policy (or repeated minor breaches) will be dealt with under the University's disciplinary procedures

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.