University of Bristol
Information Security Policy – Acceptable Use

Title	Acceptable use
Reference	ISP-09
Status	Approved
Version	2.0
Date created	October 2016
Last reviewed	July 2023
Next review	July 2024
Classification	Public

Contents

1. 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.

2. 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 Chief Digital and Information Officer are subject to this policy.

3. Policy

3.1. User Identification and Authentication

Each member will be assigned a unique identifier (userID) for their 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 must not be used as the password for any other services, including for University accounts providing privileged access (such as administrative accounts for finance or HR systems), or any external services (for example social media sites). Individual members are expected to remember their password and to change it if there is any suspicion that it may have been compromised.

University members will be asked to set up Multi-Factor Authentication (MFA) as a requirement to authenticate to University systems.

In addition to a password, authentication methods may include use of an authentication app on a mobile phone or another device, such as a USB security key, or a one-time code sent to a phone.

Information given to the University for MFA will be stored securely and only used for authentication purposes. It will be stored by the University or a contracted IT service provider and will not be provided to any third-party without the user's written consent unless the University is required to do so by law.

All administrative or highly privileged accounts must have Multi-Factor Authentication enabled where available.

3.2. Use of Email Accounts

Each member will also be assigned a unique email address for their 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.

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.

University members must not configure their University email account to automatically forward incoming mail to third-party services with which the University has no formal agreement.

Where University members are permitted to use non-University provided email clients, these must not synchronise email data with cloud services with which the University has no formal agreement.

3.3. Personal Use of Facilities

University information and communication facilities, including University networks, 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.

The use of University facilities to mine, harvest or farm cryptocurrency for non-research purposes is specifically prohibited. Any research driven activity must be approved by the appropriate Head of School.

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).

3.4. Connecting Devices to University Networks

In order to reduce the risk of malware infection and propagation, risk 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.

Any device connected to a University network must be managed effectively. Devices that do not comply with IT Services' standards for effective management are liable to physical or logical disconnection from the network without notice.

3.5. 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 the services offered by the University are unable to meet the legitimate business requirements of its members. On these occasions, members must liaise with IT Services to identify and onboard third-party solutions.

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

3.6. Unattended Equipment

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

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

3.7. 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.
- 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 activity proscribed by the Computer Misuse Act 1990.
- 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).
- Creating, storing or transmitting any material that infringes copyright.
- Creating, accessing, storing or transmitting defamatory material, obscene material, indecent material, extreme pornographic material, and prohibited images of children. In the unlikely event that there is a genuine academic need to access such material,

the University must be made aware of this in advance and prior permission to access must be obtained in writing from the Chief Digital and Information Officer.

- Creating, accessing, storing, relaying or transmitting any material with such intent to radicalise themselves or others (having regard to the University's Prevent Duty under s.26 Counter Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism). Researchers who intend to access, store or distribute such material legitimately in the course of their work must seek written permission in advance from the appropriate Research Ethics Committee, who may liaise with the University Secretary's Office. Once ethical approval has been granted, Information Security and the University Secretary's Office should be notified of this approval. If a member of the University community believes they may have encountered a breach of this provision, they should immediately contact the University Secretary.

- Using software that is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.

- Using remote access and remote control computer software that has not been approved by IT Services to remotely connect to University devices and networks.

- Using computers as servers unless registered with and authorised by IT Services.

- 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 comply with a request from an authorised person for you to change your password.

- Attempting to re-identify individuals from pseudonymised or anonymised data except when conducting a legitimate and approved business function.

Users are strongly encouraged to report any breach or suspected breach of the University's Information Security Policies to IT Services.

3.8. 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, in consultation with the University Secretary's Office, 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.

4. Further Guidance

Investigation of Computer Use Policy ISP-18:
https://www.bristol.ac.uk/infosec/policies/investigation-of-computer-use-policy/

Information Handling Policy ISP-07:

https://www.bristol.ac.uk/infosec/policies/information-handling-policy/

Outsourcing and Third Party Compliance Policy ISP-04:
https://www.bristol.ac.uk/infosec/policies/outsourcing-and-third-party-compliance-policy/

Compliance Policy ISP-03:
https://www.bristol.ac.uk/infosec/policies/compliance-policy/

JANET Acceptable Use Policy:
https://community.jisc.ac.uk/library/acceptable-use-policy

JANET Security Policy:
https://community.jisc.ac.uk/library/janet-policies/security-policy