Owner:	Chief Information Officer (CIO)
Version Number:	1.0
Date of Approval:	21 June 2019
Approved by:	University Board
Effective Date:	21 June 2019
Date of last review:	21st June 2019
Due for review:	21st June 2021

Acceptable Use Policy (AUP)

1. SCOPE AND PURPOSE

1.1 This policy directly supports the BU Information Security policy.

1.2 This policy applies to all staff[1] employed by the University and authorised users[2] that have access to information and information technology provided by or through Bournemouth University (BU).

1.3 This policy defines the way students, staff and authorised users are expected to use information and information technology which is provided by or through BU. This includes but is not limited to software, computer equipment and network connectivity. It also incorporates aspects from the Joint Information Systems Committee (Jisc) acceptable use policy which applies to all UK education and research communities who use its electronic communications networking services and facilities. The Jisc acceptable use policy, in conjunction with the Jisc security policy, is an integral part of the terms and conditions for the provision of the JANET service.

1.4 Acceptable use is that which is lawful and in accordance with the university's objectives and policies.

1.5 The use of technology (e.g. network access, computers etc.) provided by BU is permitted to fulfil and to undertake activities supporting our mission of providing education, research, and business and community engagement.

1.6 This policy sets out BU's intent and commitment to preserve the confidentiality, integrity, availability of the information it holds on behalf of its students, staff and community of stakeholders.

1.7 This policy aims to ensure BU's regulatory compliance, operational resilience, reputation and ability to sustain revenue.

1.8 This policy will be:

- communicated to students, all staff and authorised users with access to BU's information, software, equipment and connectivity;
- easily accessible by individuals;
- kept up to date

[1] This includes individuals working on a voluntary, honorary, placement or casual basis (PTHP), visiting faculty, emeritus, contractors, board members, visitors or those employed through an agency.

[2] This includes all registered students (UG, PG, full and part-time) and alumni

2. KEY RESPONSIBILITIES

2.1 The BU Board has delegated day-to-day responsibility for compliance with the policy to the Chief Information Officer.

2.2 Executive Deans of Faculties and Directors/Heads of Professional Services will be responsible for information security within their area of business and directly accountable to the Chief Information Officer (CIO) and BU Board for findings in non-compliance to this policy

2.3 Business and System owners, including academic staff, are responsible for implementing the administrative and technical controls, which support and enforce BU Information Security policy and this policy.

2.4 All students, staff and authorised users are required to read and understand this policy.

2.5 Bournemouth University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

3. LINKS TO OTHER BU DOCUMENTS

3.1 In addition to this document and the supporting set of strategic policy documents there are several BU policies which complement this policy, as follows:

- Janet Acceptable Use Policy
- BU Staff and Authorised User Information Security Policy
- Code of Practice on Freedom of Speech
- BU PREVENT Policy (arising from the Prevent Duty Guidance for HE)
- Information Classification Policy

Policy

4. THE AUP

4.1 The University's designated 'Open Access' computer resources are available to all currently enrolled students.

4.2 Access to Faculty owned specialist IT facilities, normally located within faculties, is at the discretion of the appropriate Dean of Faculty or his/her designated representative.

4.3 Equipment supplied to a student, staff member or authorised user is owned by BU.

4.4 The individual in receipt of the equipment is accountable and responsible for its use and storage until it is formally returned to the university.

4.5 Students, staff and authorised users are responsible for complying with the Information Security policies.

4.6 Where storage quotas are specified for networked file server or mail systems, users

must ensure that they manage their files and mail boxes to keep within these quotas.

4.7 It is unacceptable behaviour to send or copy restricted or confidentialinformation to un- authorized individuals or store such information on unapproved devices.

4.8 Permission is not required to remove or take away from university premises any university provided mobile devices, subject to such equipment being used solely to perform authorised university work.

4.9 All other equipment or property may not be removed or taken away from the university premises without the permission of the Dean/Director of Professional Service or nominee.

4.10 No user shall masquerade as another. Login names and passwords, which are designated for individual use, must not be shared under any circumstances.

4.11 The use of technology (e.g. network access, computers etc.) provided by BU is prohibited when the use is deemed unacceptable. Unacceptable use includes:

- any activity regarded as unlawful or potentially unlawful
- disclosing personal identifiable information and restricted or confidential information to unauthorized individuals
- creation, download, storage, transmission or display of:
    i. any offensive, obscene or indecent images, data or other material or any capable of being resolved into obscene or indecent images or unsolicited material,
    ii. material with the intent to cause annoyance,
    iii. inconvenience or needless anxiety,
    iv. material with intent to defraud,
    v. material that promotes or incites racial or religious hatred, terrorist activities or hate crime; or instructional information about any illegal activities
    vi. defamatory material (e.g. Cyber bullying),
    vii. material such that this infringes the copyright of another person,
    viii. unsolicited bulk or marketing material to users of network facilities or services unless the user of the targeted recipients has chosen to subscribe.
- deliberate unauthorized access to university equipment, facilities or property
- intending to waste BU staff or authorised users effort or JANET resources, including time and effort in supporting of those systems.
- corrupting or destroying others user data
- violating the privacy of other users
- unjustifiably disrupting the work of other users
- deliberately denying services to others (e.g. overloading resources to prevent access, also known as a denial of service)
- continuing to use an item of software or hardware after JANET Network Operations Centre or BU IT Services has requested that use cease because it is causing disruption or in breach of our regulatory compliance (e.g. licensing)
- knowingly or recklessly introducing harmful software (e.g. malware) or opening attachments from unknown or untrusted sources

- disclosing personal identifiable information and sensitive information to unauthorized individuals
- compromising passwords (e.g. by using weak passwords, reusing them, making them visible to or disclosing them to others)
- moving information or equipment off-site without authorisation (or when unencrypted)
- failing to protect computer equipment, in accordance with the Mobile Computing policy, when using it in remote environments (e.g. when travelling or working from home)
- connection of unauthorised hardware to any of the University's networks
- connection of any internet enabling device or other external link, enabling remote access to any University system without permission
- selling goods or services not personally connected to the user, or goods which do not comply with HM Customs and Excise regulations
- sell or buy goods or services, or to advertise or promote activities other than those directly related to official University business.

4.12 The list of unacceptable activities in this section is not exhaustive. The purpose is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse and potentially unlawful use of BU information and information technology.

4.13 Web content filtering blocks access to certain categories of content via BU systems: malware, illegal activity, violence, hate and racism, and cheating.
Attempts to access these sites are merely blocked; there is no attempt to identify the user or IP address and no record is made other than the overall number of attempts to access each category of site. Exemptions can be requested via SNOW (see paragraph 6.1).

4.14 BU has a responsibility to support Freedom of speech and academic freedom but within the constraints of current legislation regarding information security and data protection. Where there is a justified need to undertake activity which is contrary to this policy, explicit approval must be sought via the Policy Exception process. See Section 6 below.

4.15 BU reserves the right to use monitoring activities to protect against threats to its students, staff and to the university itself.

4.16 BU reserves the right to withdraw access privileges and report to the appropriate authority any user who uses the internet for illegal purposes.

5. PENALTIES FOR MISUSE

5.1 Minor breaches of policy will be dealt with by IT Services and HR. Deans of Faculties and Directors/Heads of Professional Services may be informed of the fact that a breach of policy has taken place.

5.2 More serious breaches of this policy may constitute a disciplinary offence for those outlined in 1.2 who will be subject to investigation under BU's disciplinary procedures. See BU Disciplinary Procedures

5.3 Any user guilty of serious or repeated breach of these rules may have their access privileges to some or all of the University's IT resources withdrawn. Such withdrawal

shall be confirmed in writing to the user and, in the case of a student, to his/her Dean of Faculty.

5.4 Bournemouth University reserves its right to take appropriate action against individuals who cause it to be involved in legal proceedings as a result of violation of its licensing agreements.

5.5 For any damage to University owned equipment a sum to cover the full cost of replacement will be payable.

5.6 The offender and the relevant Dean of Faculty will be informed if further action is to be taken. Further action may include, as a minimum, the withdrawal of all borrowing rights for a defined period.

5.7 The Procedures of the University as set out in the Student Disciplinary Procedure may be implemented in the event of damage to University property.

6. ENFORCEMENT / COMPLIANCE

6.1 Any application to depart from this policy must be submitted in writing using the Policy Exception Request form in ServiceNOW. Applications for research or other academic purposes must be supported by a written statement from the relevant Dean.

6.2 Those outlined in 1.2 may not depart from this policy until they have received written approval from the appropriate authority. If the appropriate authority refuses approval, those outlined in 1.2 may appeal to the Vice Chancellor.