Owner:	Chief Information Officer (CIO)
Version number:	5.0
Date of approval:	**23 June 2023**
Approved by:	**Audit, Risk & Governance Committee**
Effective date:	**24 June 2023**
Date of last review:	June 2024
Due for review:	June 2025

ACCEPTABLE USE POLICY

1. INTRODUCTION

This is the Bournemouth University (BU) Acceptable Use Policy, which sets out all of our requirements relating to the acceptable use of information and information technology which is provided by or through BU (the 'university').

2. SCOPE AND PURPOSE

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

2.2 This policy applies to all staff[1], students[2] and other authorised users who have access to information and information technology provided by or through BU (the 'university'). It directly supports the BU Information Security Policy and links to a number of related policies and standards which are listed in paragraph 4. It sets out BU's intent and commitment to preserve the confidentiality, integrity and availability of the information it holds on behalf of its students, staff and community of stakeholders.

2.3 The use of technology (e.g., network access, computers etc.) provided by BU is permitted to fulfil and undertake actions which support all of our education, research and practice activities. Compliance with this policy helps BU to meet its regulatory, operational and financial obligations and in turn protect its reputation.

2.4 This policy defines the way staff, students and other authorised users are expected to use information and information technology which is provided by or through BU. This includes, but not limited to, software, computer equipment and network connectivity. It is related to the Joint Information Systems Committee (Jisc) Acceptable Use Policy and Jisc Security Policy, which apply to all UK education and research communities who use its electronic communications networking services and facilities. These policies are integral elements of the terms and conditions for the provision of the Janet network which supports the UK education and research community.

[1] In addition to individuals employed by BU, 'staff' refers to those working on a voluntary, honorary, placement or casual basis (PTHP), visiting faculty, emeritus, contractors, board members, visitors and those employed through an agency.
[2] 'Students' includes all registered students (UG, PG, full-time, part-time, apprentices) and alumni

2.5 This policy will be:

- communicated to all staff, students and authorised users who have access to BU's information, software, equipment and connectivity
- easily accessible by individuals
- reviewed and updated at least once a year.

3. KEY ROLES AND RESPONSIBILITIES

3.1 All staff, students and other authorised users (see 2.1) are responsible for reading and complying fully with this policy and the associated policies, standards and controls which support it (see 4.0.) If anyone does not understand any part of the policies, or has any questions, they should ask their line manager, tutor or contact the IT Help Desk in the first instance.

3.2 The BU Board has delegated responsibility for policies governing Information Security, Data Protection and the accuracy of published information to the Audit, Risk and Governance Committee (ARG).

3.3 The Chief Information Officer (currently the Chief Operating Officer) is responsible for ensuring publication of and compliance with the policies and for ensuring that any unacceptable use of BU and Janet network services is dealt with promptly and effectively.

3.4 The Executive Deans and Directors/Heads of Professional Services are responsible for information security within their areas of responsibility and are directly accountable to the Chief Information Officer (and ultimately the Board) for any findings of non-compliance with this policy.

3.5 The Information Governance Committee (IGC) is responsible for providing appropriate oversight over the management of information and data assets (including personal data). It enables effective Information Governance (IG) and risk management, making recommendations to the University Executive Team (UET) on key decisions and risks to ensure compliance with relevant legislation and good practice. It is chaired by the Chief Information Officer.

3.6 The BU Security Review Group is responsible for overseeing the BU Security Policy which references all security-related policies and standards.

3.7 Information and System owners, including academic staff, are responsible for implementing the administrative and technical controls, which support and enforce the BU Information Security Policy and associated policies and standards (see paragraph 5).

3.8 There are also several teams across BU who provide advice and support on compliance and carry out key tasks such as responding to requests, handling security incidents, promoting good privacy, data quality, security and information management practices. These include:

- IT-Services Information Security Team - infosec@bournemouth.ac.uk
- OVC - Chief Data Officer - dpo@bournemouth.ac.uk
- Legal Services/Information Office - legalservices@bournemouth.ac.uk

4. RELATED POLICIES AND STANDARDS

4.1 There are a number of policies and standards which relate to the Acceptable Use Policy; these also apply to all staff, students and authorised users (see 2.2):

- Information Security Policy
- BU Staff and Authorised Users Information Security Policy
- Janet Acceptable Use Policy
- Code of Practice on Freedom of Speech and Academic Freedom
- Prevent Policy
- Data Protection Policy
- Asset Lifecycle Management Security Standard
- End User Computing Security Standard
- Information Management Standard
- Information Security Awareness and Training Standard
- IT External Supplier Security Standard
- Logging and Monitoring Security Standard
- Logical Access Security Standard
- Network Storage and Backup Security Standard
- Network Management Security Standard
- Project Delivery Lifecycle Security Standard
- Security Incident Management Standard
- Server Configuration Security Standard
- System Build and Delivery Security Standard
- Technical Security Architecture Standard
- Threat and Vulnerability Security Standard

4.2 The Trusted Research Agenda is a government initiative to secure the integrity of the system of international research collaboration and innovation. All universities are required by UK Research & Innovation (UKRI) to adhere to it. The Initiative spans a board range of areas, including partner suitability, managing data and cyber security, Intellectual Property (IP), commercialisation and export control. More details are here.

5. ACCEPTABLE USE POLICY

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

5.2 Access to Faculty owned specialist IT facilities, normally located within faculties, is at the discretion of the appropriate Executive Dean of Faculty or their designated representative.

5.3 Equipment supplied to a member of staff, student or other authorised user (see 2.1) is owned by BU; the individual in receipt of the equipment is accountable and responsible for its use and storage until it is formally returned to the university. Users should note that:

- the use of the internet for personal, non-work-related purposes, including email, is permitted outside working time only, subject to the following condition and to the provisions on 'Offensive Material' and 'Confidentiality' below

- material downloaded for personal purposes (eg payslips or travel documents) must be transferred to privately owned removable media and not stored on BU provided equipment.

5.4 Where storage quotas are specified for networked file server or mail systems, users must ensure that they manage their files and mailboxes to keep within these quotas.

5.5 It is unacceptable behaviour to send or copy restricted or confidential information to unauthorised individuals or store such information on unapproved devices.

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

5.7 No other equipment or property may be removed or taken away from the university premises without the permission of the Executive Dean/Director of Professional Service or their nominee.

5.8 No user is allowed to impersonate anyone else. Login names and passwords, which are designated for individual use, must not be shared under any circumstances.

5.9 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 unauthorised individuals
- creation, download, storage, transmission or display of:
    i. any offensive, obscene, or indecent images, data or other material or any capable of data being resolved into obscene or indecent images or unsolicited material;
    ii. material with the intent to cause annoyance, inconvenience or needless anxiety;
    iii. material with intent to defraud
    iv. material that promotes or incites racial or religious hatred, terrorist activities or hate crime, or instructional information about any illegal activities;
    v. defamatory material (e.g., Cyber bullying),
    vi. material such that this infringes the copyright of another person;
    vii. unsolicited bulk or marketing material to users of network facilities or services unless the user of the targeted recipients has chosen to subscribe
- deliberate unauthorised access to university equipment, facilities, or property
- intending to waste BU staff or authorised users' effort or Janet/Jisc resources, including time and effort in supporting of those systems
- storing of large amounts of material downloaded for personal purposes on BU systems
- excessive use of BU printing facilities for printing downloaded materials
- 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 BU IT Services or the Janet Network Operations Centre 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 unauthorised 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 End User Computing Security Standard, 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:
    - where the BU/Janet network is being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network will be regarded as unacceptable use of Janet. Any activity as described above, and where applied either to a user of that network, or to an end system attached to it, will also be regarded as unacceptable use of Janet.
    - any deliberate or persistent breach of industry good practice (as represented by the current standards of the London Internet Exchange) that is likely to damage the reputation of BU or Jisc will also be regarded prima facie as unacceptable use of BU/Janet network.
- 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 HMRC regulations
- selling or buying goods or services, or to advertise or promote activities other than those directly related to official university business.

5.10 The list of unacceptable activities in paragraph 5.9 is not exhaustive, but is intended to illustrate clearly those activities most commonly associated with the abuse and potentially unlawful use of BU information and information technology.

5.11 Online calls/video calls and messaging may be used for legitimate BU purposes such as meetings, presentations, or collaboration sessions. All users are expected to conduct themselves in a professional manner. Personal use of video call platforms during work hours should be limited to essential communication and must not interfere with job responsibilities or productivity. All users must exercise caution when sharing sensitive or personal information over calls or messaging and ensure compliance with this policy (see 5.9).

5.12 Recording staff meetings is not allowed unless there is a specific need for reasonable adjustments (see Accessibility Guidance) and agreement from the attendees.

5.13 Individuals must not knowingly access nor store on any University system, download from the Internet, or transmit using telephone, written letter or electronic mail any material or message which may reasonably be offensive or obscene. Any member of staff who may need to access such material for professional, academic, research must obtain the written authorisation of the relevant Executive Dean of Faculty or Director/Head of Professional Service first. Where such authorisation has been given, care must be taken to ensure that colleagues, students, or other persons do not inadvertently witness or gain access to such material. Possession of indecent images of children under age 18 is a criminal offence, and anyone found to be in unauthorised possession of such material will be reported to the police.

5.14 All university core business activities (education, research, practice and administration) that require the use of IT systems (e.g. hardware, software, enterprise solutions and cloud services), must be carried out using authorised IT Systems via IT Services. The use of authorised cloud services on personal devices (for BU purposes) is acceptable as long as no data is removed from the service to be stored on non-BU-managed devices without explicit consent from a member of the relevant Executive Dean or Director/Head of Professional Service. The use of personal cloud services (such as non-BU OneDrive, Google Drive, Google Docs & Dropbox) for university business is prohibited.

5.15 Web content filtering blocks access to certain categories of content via BU systems: illegal activities, child abuse content, hate speech, terrorism and violent extremism and extreme content. 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 Hornbill (see paragraph 6.1).

5.16 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.

5.17 BU reserves the right to use monitoring activities to protect against threats to its students, staff, other authorised users and to the university itself.

5.18 BU reserves the right to withdraw access privileges and report any user who uses the internet for illegal purposes to the appropriate authority, such as the Director of Human Resources, Director of Student Services or the police.

6. PENALTIES FOR MISUSE

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

6.2 More serious breaches of this policy may constitute a disciplinary offence for staff, students or other authorised users and will be subject to investigation under BU's disciplinary procedures.

6.3 Any user who is found guilty of serious or repeated breach of this policy 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 their Executive Dean of Faculty or to the relevant Executive Dean or Director/Head of Professional Service if the individual is a member of staff.

6.4 BU 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.

6.5 The full cost of replacement will be charged to anyone who wilfully or deliberately damages university-owned equipment. The offender and the relevant Executive Dean of Faculty or Director/Head of Professional Service will be informed if further action is to be taken, such as invoking the relevant disciplinary procedure. Further action may include, as a minimum, the withdrawal of all borrowing rights for a defined period.

7. ENFORCEMENT AND COMPLIANCE

7.1 No members of staff, students or other authorised users may depart from this policy unless or until they have received written approval from the relevant Executive Dean of Faculty or Director/Head of Professional Service. If the appropriate authority refuses approval, they may appeal to the Vice Chancellor.

7.2 Any application to depart from this policy must be submitted in writing using the IT Policy Exemption request form in Hornbill. Applications for research or other academic purposes must be supported by a written statement from the relevant Executive Dean.