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

INFORMATION SECURITY POLICY

1. INTRODUCTION

This is the Bournemouth University (BU) Information Security Policy, which sets out all of our requirements and expectations relating to the handling of information in order to preserve the confidentiality, integrity and availability of the information held on behalf of students, staff and other stakeholders. Information is a critical asset which supports all of our activities; it must be managed accurately, efficiently, securely and legally, in accordance with all of our relevant policies, procedures and standards.

2. SCOPE AND PURPOSE

2.1 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 is supported by a number of related policies and standards (see paragraph 5).

2.2 'Information' means all information that is owned, stored or processed by, or on behalf of, BU via computerised information systems, paper records and any other form including photographs. Information systems that hold BU data are in-house, off-site, in the cloud or developed by a third party.

2.3 'Storage' includes personal computers, laptops, mobile phones and other mobile devices such as USB memory sticks. Information can be processed or used by individuals on and off-campus, including at home, while travelling and when based in external organisations.

2.4 'Data' serves as the raw material from which information is derived. Data can include various types of digital assets, such as personal identifiers (e.g. name), financial records, intellectual property, and operational data. Information is structured, meaningful, and relevant to a specific purpose or context. Information security is essential for safeguarding both data and information from threats and risks, ensuring their confidentiality, integrity and availability, and supporting the BU objectives and its reputation.

---

[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

3. KEY ROLES AND RESPONSIBILITIES

3.1 All staff, students and other authorised users (see 2.1) are responsible for complying fully with this policy and the associated policies, standards and controls which support it (see *5)

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 compliance with the policies.

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 There are also several teams across BU who provide advice and support on compliance and carry out key tasks like 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. POLICIES

4.1 We are committed to implementing security controls that conform to best practice, as set out in the ISF Standard of Good Practice for Information Security and ISO 27000 Information Technology, Security Techniques and Information Security Management Systems.

4.2 This policy is supported by a number of related policies and standards (see paragraph 5). These are regularly reviewed by the Information Governance Committee to ensure that they remain appropriate in the light of any relevant changes to the law, university policies, contractual obligations, technological developments, emerging threats and near-miss or actual incidents. They are also reviewed as part of the annual report to the Audit, Risk & Governance Committee.

4.3 These policies, standards and supporting information are shared with staff, students and other authorised users (via the communication updates and staff

and student intranet pages following approval of the annual report (in June of each year) and following any significant change or incident.

4.4 All staff (and PGR students) must undertake mandatory information security training; this is provided via online modules on KnowBe4. Completion rates are monitored by the Chief Information Officer and shared with members of the University Leadership Team (ULT) for action where necessary.

4.5 Information systems should be classified in a way that indicates their importance to BU. Appropriate owners are appointed for all critical and sensitive information and information systems.

4.6 Information system owners will undertake security risk assessments on all of their information systems on a regular basis, before any major change and after any near-miss or actual incident, in order to identify potential risks to the system and its information, and determine the controls needed to manage those risks.

4.7 Arrangements with third parties which involve accessing, processing, communicating or managing BU's information or information systems should cover all relevant security requirements, and be included in contractual arrangements. All third parties must be made aware of their obligation to comply with this and associated policies, including the IT External Supplier Security Standard.

4.8 The university will establish and maintain appropriate contact with both internal and external agencies regarding this policy and continuing relevance, e.g. business partners, law enforcement authorities, regulatory bodies, network, and telecommunications operators.

4.9 This paragraph is redacted.

4.10 All suspected or known breaches of this policy will be considered a security incident and must be reported to the IT Helpdesk on 01202 965515 (freephone 0808 1962332) option 1 immediately, or via this online form. This is available 24/7, all year-round. Any other queries or concerns should be addressed to the Information Security Manager and the Data Protection Officer. The Data Protection Officer must be informed of all incidents, confirmed data breaches, near misses and concerns.

5. RELATED POLICIES AND STANDARDS

5.1 This section provides a brief overview of the related policies and standards, which contain high-level descriptions of expectations and principles. These also apply to all staff, students and authorised users (see 2.1).

5.2 The Acceptable Use Policy (AUP) defines BU's rules on how individuals can use technology, including software, computer equipment and network connectivity provided by the university.

5.3 The Data Protection Policy is intended to ensure that all staff and other relevant individuals who process Personal Data for BU purposes or have access to BU

systems are properly informed about BU's obligations under the Data Protection Legislation and their role in enabling BU to comply with those obligations.

5.4 The Data Breach Management Plan sets out actions required in the case of a suspected or actual data breach.

5.5 The Payment Card Industry Data Security Standard (PCI-DSS) Policy sets out the requirements for protecting the security of all credit and debit card payments received and processed by the university, which are governed by the Payment Card Industry Data Security Standard (PCI-DSS) (the Standard).

5.6 The following standards are based on best practice and set out roles, responsibilities and expectations regarding compliance:

- 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

6. ENFORCEMENT AND COMPLIANCE

6.1 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.

6.2 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.