BUCKINGHAMSHIRE
NEW UNIVERSITY

EST. 1891

Information Security Policy

Contents

Approved by:	Digital Experience Steering Group	**Date first published:**	Jun-2015
Version:	2.3	**Date updated:**	Jun-2024
Owner:	Director of Digital & Technical Services	**Review Date:**	Jun-2026

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the University Secretariat.

Purpose

1 The purpose of information security is to protect information and information systems from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments or business opportunities. At all times the cost effectiveness and fitness for purpose of these measures will be considered.

2 By using Information and Communication Technology (ICT) staff, students and authorised visitors at Buckinghamshire New University (BNU) have the ability to create and access a wide range of electronic information. This Information Security Policy is concerned with creating and maintaining an environment that protects these information resources from accidental or intentional unauthorised use, modification, disclosure, or destruction.

3 BNU is committed to safeguarding the integrity, confidentiality, and availability of University information and will protect the interests of the University, its students, its staff, its partners, and the general public.

- **Confidentiality**: Ensures that information is accessible only to those authorised to have access
- **Integrity:** Safeguards the accuracy and completeness of information and processing methods
- **Availability**: Ensures that authorised users have access to information and associated assets when required

4 The following principles guide the development and implementation of BNU's information security policies and practices:

a) Information is:

- A critical asset that must be protected; and
- Restricted to authorized personnel for authorized use.

b) Information security is:

- The cornerstone of maintaining public trust;
- A business issue — not a technology issue;
- Risk based and cost effective;
- Aligned with University priorities, industry-prudent practices, government requirements, and all legal and regulatory requirements;
- Directed by policy but implemented by business owners; and
- Everybody's business.

5 This Information Security Policy is only part of a range of controls required for an effective Information Security Management System and should be read in conjunction with other policies, processes and procedures relating to the use of information and communications and relevant legislation. Key relevant University policies are listed under Key Relevant Documents.

Applicability and Scope

6 This policy applies to all information processing facilities and information processed and stored in, or on, the assets of BNU either owned or operated by the university or connected to the network by a third party.

7 This policy applies to all University students, staff, partners, affiliates, contractors and third parties who have access to University's premises, equipment, and/or systems.

8 Information Security is concerned with creating and maintaining an environment that protects the University's information resources from accidental or intentional unauthorised use, modification, disclosure, or destruction with the objective to:

- Protect information resources critical to the University;
- Protect information as mandated by laws, regulations, directives, law enforcement and judicial processes;
- Protect the personal information and privacy of all users including staff, students, affiliates and partners;
- Reinforce the reputation of the University as an institution deserving of public trust;
- Comply with due diligence standards for the protection of information resources; and
- Assign responsibilities to relevant University officers, executives, managers, employees, contractors, partners, and vendors.

9 BNU will use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives.

10 ISO 27001:2022: Information Security Management will be used as a guide for determining policy and managing security. Other schemes such as Cyber Essentials will be referenced as required.

11 This document is the University's policy for meeting its requirements under the Freedom of Information Act 2000 (FOIA) and incorporates guidance from the Information Commissioners' Office (ICO).

12 The policy provides a framework for compliance and is supported by appropriate procedures and guidance documents to provide advice and maintain good practice.

Responsibilities for Information Security

13 Everyone who makes use of University systems and information has a responsibility for protecting those assets. Individuals must, at all times, act in a responsible and professional way in this respect, and shall refrain from any activity that may jeopardize security.

14 It is the responsibility of each individual to ensure that they understand and comply with this policy and any associated policies, processes, procedures or codes of practice.

15 Staff with supervisory responsibility should make their supervised staff or students aware of best practice.

16 Staff and students who process or who are responsible for the processing of personal data, as defined in the University's Data Protection Policy, are additionally required to understand and comply with all obligations placed upon them under agreements with external parties, including but not limited to information security, integrity and confidentiality.

Compliance with Legislation

17 Every member of University staff and every student has an obligation to abide by all UK legislation. Of particular importance in this respect are the Computer Misuse Act 1990, the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Terrorism Act 2006 and the Counter Terrorism and Security Act 2015

18 Relevant legislation is referenced in supporting policies and guidelines.

Breaches of Security

19 The Data Protection Officer will advise on what steps should be taken to avoid incidents or minimize their impact, and identify action plans to reduce the likelihood of recurrence.

20 Any individual suspecting that the security of a computer system or information system has been, or is likely to be, breached should inform the IT Service Desk.

21 In the event of a suspected or actual breach of security, the Data Protection Officer may, after consultation with the relevant system owner, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

22 Where a breach of security involving either computer or paper records relates to personal information, the Data Protection Office must be informed, as there may be an infringement of the Data Protection Act 2018 which could lead to civil or criminal proceedings. It is vital, therefore, that users of the University's information systems comply, not only with this policy, but also with the Data Protection Policy and policies and procedures, details of which are available on the University website.

23 All physical security breaches should be reported to the University Security team.

Policy awareness

24 Line managers are responsible for ensuring that online information security training is completed and that their supervised staff or students are aware of and understand this policy.

25 Students are required to comply with this and all supporting Information Security Policies including such additions and amendments that may be made from time to time.

26 All University affiliates, partners and third parties granted access to the University network will be advised of the existence of this policy statement and the availability of the associated policies procedures, processes, standards and guidance notes which are published on the University website.

Enforcement

27 DTS Directorate staff or their appointed agents will monitor information systems and the network to detect unauthorised activity, identify potential weaknesses and pro-actively prevent security incidents. All monitoring will be completed in accordance with approved university policies and procedures.

28 Failure of an individual student or member of staff to comply with this policy and any supporting policies may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken.

29 Failure of a contractor to comply with this policy and any supporting policy could lead to the cancellation of a contract.

Key Relevant Documents

30 Supporting policies, processes, procedures, standards and guidance notes are available on the University website. Staff, students, contractors and other third parties authorized to access the University network to use University systems and facilities, are required to familiarize themselves with these and to work in accordance with them.

31 Key University Polices include, but are not limited to the following:

- Acceptable Use Policy
- Bring Your Own Device Policy
- Data Protection Policy
- Email Policy
- Information Classification Policy
- Monitoring Computer and Network Use Policy
- Password and Multifactor Authentication Policy
- Records Management Policy

Table of Definitions

DPO	Data Protection Officer
FOIA	Freedom of Information Act
ISMS	Information Security Management System
ICO	Information Commisioners Office
ISO 27001	International Standard for Information Security
UK GDPR	UK General Data Protection Regulation

Appendix: Equality Impact Assessment

1. What is changing and why?				
This core information security policy provides the framework to help make sure that the data held and processed by the University is managed with the appropriate standards to keep it safe. This policy was first introduced in June 2015 and has been reviewed in accordance with the review schedule.				
2. What do you know?				
This policy aims to ensure that all BNU staff and students are fully aware of their responsibilities in relation to information security. This will help to ensure that the personal information of staff, students, service users and stakeholders in general will be processed fairly and lawfully in accordance with the requirements of the Data Protection Act 2018 and UK GDPR.				
3. Assessing the impact				
	Could benefit	**May adversely impact**	**What does this mean?** *Impacts identified from what you know (actual and potential)*	**What can you do?** *Actions (or why no action is possible) to advance equality of opportunity, eliminate discrimination, and foster good relations*
a) How could this affect different ethnicities? *Including Gypsy, Roma, Traveller, Showmen and Boaters, migrants, refugees and asylum seekers.*	☐	☐	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	
b) How could this affect cisgender and transgender men and women (including maternity/pregnancy impact), as well as non-binary people?	☐	☐	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	
c) How could this affect disabled people or carers? *Including neurodiversity, invisible disabilities and mental health conditions.*	☐	☒	It is not considered that the policy itself will impact on individuals with this protected characteristic. It is acknowledged that different disabilities will require a tailored approach to elements of how the policy is implemented.	Whilst it is not considered that the policy will have an impact, the intention is that the plans and projects that stem from the policy will have separate EIAs which will identify areas with a positive or negative impact that may require mitigation.
d) How could this affect people from different faith groups?	☐	☐	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	
e) How could this affect people with different sexual orientations?	☐	☐	Neutral:	

			It is not considered that the policy itself will impact on individuals with this protected characteristic.	
f) How could this affect different age groups or generations?	□	□	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	It is noted that people of different ages will have mixed technical ability and to that end, the plans and projects that stem from the policy will have separate EIAs which will identify areas with positive or negative impact that may require mitigation.
g) How could this affect those who are married or in a civil partnership?	□	□	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	
h) How could this affect people from different backgrounds such as: socio-economic disadvantage, homeless, alcohol and/or substance misuse, people experiencing domestic and/or sexual violence, ex-armed forces, looked after children and care leavers.	□	□	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	
i) How could this affect people with multiple intersectional experiences?	□	□	Neutral: It is not considered that the policy itself will impact on individuals with this protected characteristic.	
4. Overall outcome				
No major change needed ☒	Adjust approach □	Adverse impact but continue □	Stop and remove □	
5. Details of further actions needed				
None required				
6. Arrangements for delivery and future monitoring				
The Director of DTS is responsible for ensuring the policy is reviewed on an annual basis.				
7. Completed by:	Jenny Horwood	Technical Project Manager	**Date**	**01/06/2022**
8. Signed off by:	Nicholas Roussel-Milner	Director DTS	**Date**	**23/02/2023**

High Wycombe Campus
Queen Alexandra Road
High Wycombe
Buckinghamshire
HP11 2JZ

Aylesbury Campus
59 Walton Street
Aylesbury
Buckinghamshire
HP21 7QG

Uxbridge Campus
106 Oxford Road
Uxbridge
Middlesex
UB8 1NA

BNU based at
Pinewood Studios

Pinewood Studios
Pinewood Road
Iver Heath
Buckinghamshire
SL0 0NH

Missenden Abbey
London Road
Great Missenden
Buckinghamshire
HP16 0BD

Telephone: 01494 522 141

BucksNewUni

BucksNewUni

BucksNewUni

BucksNewUniversity

If you have any queries about this policy, please contact the School or Directorate responsible for the policy