BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891

Monitoring Computer and Network Use Policy

Contents

Approved by:	Digital Experience Steering Group	**Date first published:**	Aug-2018
Version:	2.0	**Date updated:**	Oct-2023
Owner:	Director DTS	**Review Date:**	Oct-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 There are circumstances where the university may monitor or record communications made using its IT and telecommunication systems, or examine material stored on those systems. This document sets out Buckinghamshire New University's (BNU) policy in respect of such activity.

2 All users of IT services provided by BNU should be aware that usage, including internet and email use, may be logged and monitored, and that the University may access electronic information, whether stored or in transit. This is done in order to comply with various pieces of legislation, for example, the Data Protection Act 2018 (DPA), the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications Regulations 2000.

3 This policy provides information on the circumstances in which it is permissible for the University to access information stored in User Accounts, or to monitor use of IT systems and services including internet use.

Applicability and scope

4 This policy applies to anyone using IT systems and services (hardware, software, data, network access, third party services, online services or IT credentials) provided or arranged by the university. This applies to information associated with personal and non-personal user accounts, and includes but is not limited to:

- Email files, including student email;
- Files contained in individual or shared storage locations associated with user accounts issued to staff, students, and other authorised users e.g. OneDrive, SharePoint, G:Drive and S:Drive;
- Internet use, when using the University network, wi-fi or internet (JANET) connection; and
- The use of social media.

5 This policy applies to 3rd party and personal devices that are connected to the University's network to access IT systems and services.

6 This policy should be read in conjunction with the University's Acceptable Use Policy. All use of BNU IT systems and services must comply with the University Acceptable Use Policy and the Jisc Acceptable Use Policy.

Routine monitoring

7 Monitoring for routine operational reasons is completed to ensure that IT systems and services are performing properly. This normally involves only aggregated anonymous data that does not identify individuals or the contents of files or communications. This data may be used for data analytics.

8 Monitoring and logging usage of University IT systems and services and accessing data in user accounts may only be undertaken by specific members of staff as a recognised part of their normal duties, for example:

- email postmasters may examine misaddressed messages in order to redirect them as necessary, or check email subject lines for malicious content;
- system and network managers may investigate which system and/or individual is the source of a denial of service attack.

This work must be:

- Approved;
- For legitimate business reasons;
- Justifiable;
- Fair;
- Proportionate;
- Not unnecessarily intrusive; and
- Compliant with UK legislation.

9 Information on University IT equipment and networks, including mobile phones, may be routinely monitored to:

- Support detection or prevention activities that are in breach of University policy;
- Comply with legislation;
- Support detection or prevention of activities that are illegal;
- Defend against attacks against its systems or data;
- Identify or investigate an operational problem or monitor for correct operation;
- Investigate suspected unauthorised access to or use of systems; and
- Perform monitoring or support activities with consent of the subject.

10 User-specific information may be routinely monitored or logged by authorised staff with respect to:

- Login and logout events and locations;
- System resource usage;
- Software usage;
- Software auditing to support compliance;
- Network bandwidth usage;
- Network bandwidth usage and traffic patterns;
- Power consumption;
- Detection of email spam;
- Detecting security vulnerabilities;
- Identifying and controlling security threats; and
- Detecting inappropriate content, which may include material which is obscene, violent, illegal, damaging to the University or otherwise in breach of University policy.

11 Routine monitoring may make use of automated systems which scan user files and communications for an approved purpose.

Monitoring for legal and policy compliance

12 In special circumstances authorised University staff may access and examine the content of any data stored in, or being transmitted by, University IT systems and services. This includes examining the content of data files and communications which should otherwise be treated as confidential and therefore goes beyond what is permitted in routine monitoring.

13 Monitoring or access to stored material to investigate legal or policy compliance may only be carried out with written authorization from one of the following (or their deputies) as appropriate:

- Director of Human Resources (in pursuance of staff disciplinary matters);

- Academic Registrar (in pursuance of student disciplinary matters);
- Data Protection Officer (in pursuance of data protection issues); and
- Head of Directorate or Academic School (in relation to systems under his/her authority).

Email monitoring

14 The University maintains the right to monitor the use of email accounts to ensure compliance with University policies. Any monitoring will be done in compliance with the Telecommunications Regulations 2000.

15 The University maintains the right to apply automatic message monitoring, filtering and rejection systems as appropriate and deny transmission of messages with content that is unacceptable, harmful or in breach of University policy.

16 Any email identified with a very strong spam score will be discarded prior to delivery to the user's mailbox. Attachments identified as a potential security risk may be removed

17 BNU 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. Users must not use their email account to create, download, store or transmit unlawful material or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material.

18 Under Prevent duty guidance the University has an obligation and right to monitor emails for possible evidence of criminal activity or activity contrary to the Prevent statement in section 23. Authorised system administrators may provide the evidence of such monitoring to law enforcement officials.

Access to web sites

19 All individuals are responsible for ensuring that their internet use is compliant with University policies and the law.

20 All access to the Internet is logged and monitored. If monitoring reveals possible evidence of criminal activity, or a repeated breach of the University or Jisc acceptable use policies by attempting to access these sites or similar sites a disciplinary investigation will be instigated, and the police may be notified (where relevant).

21 Websites which are recognised as being harmful to computer systems or those known to be used to host harmful software or distribute phishing emails linked to malicious intent will be blocked to protect university systems and information.

22 BNU has a statutory obligation under the Prevent responsibilities of the Counter-Terrorism and Security Act 2015 to have "due regard to the need to prevent people from being drawn into terrorism". Under Prevent the University has a responsibility to review the use of filters as a means of restricting access to material promoting terrorism.

23 If you attempt to access a site that is in the 'block' category of the web filter a message will appear on your web browser. If you need access to the site, please contact the IT Service Desk, and the request will be reviewed and if appropriate the block will be removed.

24 Where an individual requires access to Internet sites that are blocked by a web filter or may contravene University or Jisc acceptable use policies (such as pornography, extremism) as part of a

teaching or research proposal, clearance must be obtained from the University Ethics Panel. This ensures that any actions identified through monitoring of internet usage can be tied to valid and approved activities.

Network scanning

25 The University reserves the right to conduct scans of the network in order to determine what devices are connected to it and what network services are running on the device. If there are reasonable grounds to believe that a device connected to the network may present a security risk or contravene University policies, DTS may take action to prevent the device connecting to University resources until the issue is resolved.

26 The University may also conduct (or commission from third parties) penetration tests or vulnerability scans in order to identify potential security weaknesses.

Use of information gathered from monitoring

27 Any monitoring information that is collected in relation to a student or member of staff may be used in a disciplinary investigation, for example where there is inappropriate use of the internet or e-mail. Information collected may also be passed to relevant authorities if there are any criminal proceedings to which it relates.

28 Monitoring information may be used for training purposes, for example telephone training.

29 Monitoring information may also be used for analytical purposes to plan and deliver IT and telecommunications services.

30 The university will provide access to third parties where there is a legal reason for doing so. For example, information may be requested as part of legal proceedings including Freedom of Information Act, Data Protection Act 2018 or Regulation of Investigatory Powers Act.

Retention of information

31 Information gathered during routine monitoring operations will be kept according to the University's Records Retention Schedule

Enforcement

32 Any actual or suspected breach of this policy must be reported to the Director of DTS via the Service Desk. The Director of DTS will take appropriate action and inform the relevant internal and external authorities.

33 Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

Key relevant documents

34 This policy should be read and understood in the context of other Buckinghamshire New University Policies which together form the Information Security framework. Key documents include:

- Applicable Laws and Regulations
- Acceptable Use Policy

- BYOD Policy
- Data Protection Policy
- Records Management Policy and Records Retention Schedule
- Social Media Policy

Appendix: Equality Impact Assessment

1. **What is changing and why?**				
This policy has been reviewed and updated according to the review schedule.				
2. What do you know?				
This policy is a factual and procedural document, providing details on how the University monitors the use of computers and network by staff, students and other users. It addresses compliance with laws and regulations and the need to protect the University's information, balanced with the need to protect the rights of learners, staff and partners.				
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.*	☒	☐	This policy does not distinguish between or affect differently people of different ethnicities. It protects the interest of all users by ensuring that university resources are used in accordance with university policy and wider legislation.	
b) How could this affect cisgender and transgender men and women (including maternity/pregnancy impact), as well as non-binary people?	☒	☐	This policy does not distinguish between or affect differently cisgender and transgender men or women or non-binary people. It protects the interest of all users by ensuring that university resources are used in accordance with university policy and wider legislation.	
c) How could this affect disabled people or carers? *Including neurodiversity, invisible disabilities and mental health conditions.*	☒	☐	This policy does not distinguish between or affect differently those with a disability or who are carers. It protects the interest of all users by ensuring that university resources are used in accordance with university policy and wider legislation.	The policy is available on the BNU website therefore is available in different fonts, text size and through assistive technology.
d) How could this affect people from different faith groups?	☐	☐	It is not envisioned that there will be any direct impact on people from different faith groups as the policy applies to everyone. Therefore, there should be no difference in how individuals who share this protected characteristic are treated by the policy.	
e) How could this affect people with different sexual orientations?	☐	☐	It is not envisioned that there will be any direct impact on people with different sexual orientation as the policy	

			applies to everyone. Therefore, there should be no difference in how individuals who share this protected characteristic are treated by the policy.	
f) How could this affect different age groups or generations?	☒	☐	This policy does not distinguish between or affect differently people from different age groups or generations. . It protects the interest of all users	
g) How could this affect those who are married or in a civil partnership?	☐	☐	It is not envisioned that there will be any direct impact on people who are married or in a civil partnership as the policy applies to everyone. Therefore, there should be no difference in how individuals who share this protected characteristic are treated by the policy.	
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.	☒	☐	This policy does not distinguish between or affect differently people from different backgrounds. It protects the interest of all users.	
i) How could this affect people with multiple intersectional experiences?	☒	☐	This policy applies to all in the same way therefore there will not affect those with multiple intersectional experiences.	This is a factual and procedural document however it can be considered to support equality and diversity in so much as it makes numerous references to the need to monitor the use of University resources for any activity likely to cause annoyance, inconvenience or needless anxiety.

4. Overall outcome			
No major change needed ☒	Adjust approach ☐	Adverse impact but continue ☐	Stop and remove ☐

5. Details of further actions needed
The inappropriate use of the Policy will be managed in accordance with the University's policies and procedures and reported to external bodies when appropriate.

6. Arrangements for delivery and future monitoring
The policy will be reviewed every three years. The Director of Digital & Technical Services is responsible for reviewing the policy.

7. Completed by:	Jenny Horwood	Technical Project Manager	**Date**	04-Oct-23
8. Signed off by:	Nicholas Roussel-Milner	Director DTS	**Date**	15/01/2023

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