BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891

MONITORING POLICY

bucks.ac.uk

Contents

Introduction **2**

Policy Scope **2**

Policy Intent **2**

Policy Provisions and Principles **2**

Routine monitoring 2

Monitoring for legal and policy compliance 3

Email monitoring 3

Access to web sites 4

Network scanning 4

Use of information gathered from monitoring 4

Retention of information 4

Compliance **4**

Key Relevant Documents **4**

Approved by:	**ITSC**	Date first published:	**Aug-2018**
Version No.	**1.0**	Date updated:	**Jun- 2019**
Owner:	**IS&T**	Review Date:	**May-2021**

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

Introduction

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 Bucks New University's policy in respect of such activity.

2 All users of IT services provided by Bucks New University 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 in order to comply with the law and applicable regulations and to ensure appropriate use of the University IT systems and services. Any such activity will comply with applicable UK legislation.

Policy Scope

3 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 storage locations associated with user accounts issued to staff, students, and other authorised users e.g. G:Drive, S:Drive and OneDrive
- Internet use, when using the University network, wi-fi or internet (JANET) connection.

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

Policy Intent

5 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.

Policy Provisions and Principles

Routine monitoring

6 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.

7 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
- Compliant with UK legislation

8 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
- Perform monitoring or support activities with consent of the subject

9 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
- Detecting inappropriate content, which may include material which is obscene, violent, illegal, damaging to the University or otherwise in breach of University policy

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

Monitoring for legal and policy compliance

11 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.

12 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)
- Head of Directorate, Department or Academic School (in relation to systems under his/her authority).

Email monitoring

13 Automated tools will be used to scan incoming and outgoing email for spam and malware. Email content is not otherwise routinely monitored.

14 Any email identified with a very strong spam score will be discarded prior to delivery to the user’s mailbox.

15 Attachments identified as a potential security risk may be removed.

Access to web sites

16 All individuals are responsible for ensuring that their internet use is compliant with University policies and the law. Access to web sites is not normally blocked however, the University reserves the right to block access to web sites where it is deemed necessary, for example for legal or compliance reasons, or to protect users of the University.

Network scanning

17 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, IS&T may take action to prevent the device connecting to University resources until the issue is resolved.

18 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

1 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.

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

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

4 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

5 Information gathered during routine monitoring operations will be kept according to the universities Records Retention Schedule.

Compliance

6 Failure to comply with this policy may be dealt with in accordance with the university’s disciplinary procedures.

Key Relevant Documents

IT Regulations of Use
Information Security Policy
Network Access Policy
Records Lifecycle Management Scheme

Revision History

Version	Status	Name	Reason for change	Date
0.1	Draft	JH	Initial document	22 Aug 18
1.0	Final	JH	Updates	Jun 19