Email Policy

Contents

Purpose

1 Buckinghamshire New University recognises that email and instant messaging are important communication tools for both staff and students. Email systems are provided to support the teaching, learning, research and approved business activities of the University.

2 This policy provides guidance on secure, acceptable and appropriate use of the University's email and related services, systems and facilities.

Applicability and Scope

3 The policy applies to all Users who are issued with a Buckinghamshire New University email account this includes students, staff, partners, affiliates, contractors and third parties.

4 The policy applies to all University students, staff, partners, affiliates, contractors and third parties who use Instant Messaging and social media applications provided by Buckinghamshire New University

5 This policy provides guidance about acceptable use, for the purpose of sending or receiving email messages and attachments and the sending and receiving of Instant Messages (chat) using IT facilities (hardware , software and networks) provided by Buckinghamshire New University.

6 This policy describes the standards that users are expected to observe when using University facilities for email and chat, and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

Use of email

7 The University uses electronic mail to communicate official University information of many kinds to Staff, Students and others. Users are responsible for reading and responding to their email on a frequent and regular basis, since some official communications may be time sensitive.

8 Users are responsible for setting up an automatic out of office reply through Outlook when they are away from the University. This should include alternative contact details for urgent enquiries.

9 The sending of insulting, abusive or otherwise offensive messages or material is not permitted. Similarly, no information should be transmitted internally or externally which is defamatory, which brings the University into disrepute, or which contravenes laws, University policy and conventions on equal opportunities. Employees or students who receive emails with such content from other employees or students of the University or external parties should report the matter to their line manager or academic supervisor

10 Any information which the University holds is potentially disclosable to a requester under any of the applicable Data Protection Legislation. This includes emails and chat.

11 Users need to be sure that they are not breaching any Data Protection Legislation and are complying with the information handling procedures when using email. This could include but is not limited to:
- Passing on personal information without consent from the data owner;
- Keeping personal information longer than necessary; and
- Sending personal information to a country outside the EEA.

12 Emails form part of the official records of the University. Emails are treated as a legal form of written communication , and care should be taken to avoid communicating information that may be regarded as unsuitable or unacceptable

13 Staff may not automatic use personal email accounts instead of a University staff email account to conduct University business, or automatically forwarding emails from a staff email account to a personal account.

14 University email should not be used as a permanent document storage or archiving facility.

15 Inboxes should be cleaned up periodically to remove unwanted emails (junk and obsolete) permanently. Where email messages need to be retained for long periods, these should be saved on the appropriate network drive and the emails deleted from the inbox.

Security and Privacy

16 The University makes every effort to secure its computer systems, networked resources, and email accounts, but cannot guarantee the infallibility of these systems to unauthorized intrusion, nor the authenticity of the sender of an electronic communication. For this reason email is not appropriate for transmitting personal, confidential or sensitive information of any kind.

17 Email should be used carefully when transmitting personal data. Any email containing personal information about an individual may be liable to disclosure to that individual under the Data Protection Legislation. This includes comments and opinions, as well as factual information. This must be borne in mind when writing emails, and when keeping them. Emails which do not contain personal information but contain other information that may be classified as confidential or sensitive may be liable to disclosure under the Freedom of Information Act 2000.

18 The University does not recognise any rights of email users to impose restrictions on disclosure of emails held in the University's system. Emails may be disclosed under the Freedom of Information Act or Data protection Legislation, as part of legal proceedings (e.g. tribunals) or disciplinary investigation proceedings. Users are responsible for all actions relating to the use of their University IT Credentials and email accounts and should therefore make every effort to ensure no other person has access to their accounts.

19 Users are responsible for keeping their email passwords confidential, and should never share this information with others, including friends and family members.

20 If an employee is absent the University reserve the right to access accounts in order to access emails and files to ensure business continuity.

Monitoring

21 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.

22 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 the terms of the policy.

Enforcement

23 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.

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

Key Relevant Documents

25 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

- Data Protection Policy

- Information Security Policy

Table of Definitions

IT Facilities	Hardware, software, data, network access, third party services, online services or IT credentials provided or arranged by Buckinghamshire New University.
IT Credentials	Your institutional login, often referred to as your Username, or any other token (email address, smartcard, dongle) issued by Buckinghamshire New University to identify yourself when using IT facilities.
Staff	Staff are salaried members of the University or contracted individually by the University to provide a service.
Student	A person pursuing any course of study in the University.
Visitors	A visitor is anyone, not a member of staff or student, requiring access to University premises or services.

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