
Acceptable Use Policy

Purpose

This summarizes the key responsibilities and required behaviour of **all** students of the University of Bolton computer and information systems.

Policy

All students are required to adopt procedures and practices that ensure the security, integrity and protection of information created and held by The University of Bolton, and to abide by the University's rules for the use of computer systems.

Applicable statutory regulations

The management of information security and the use of computers at the University of Bolton are framed by UK legislation including:

- Data Protection Act (1998)
- Counter-Terrorism and Security Act 2015
- Regulation Of Investigative Powers Act (2000)
- Freedom Of Information Act (2000)
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- PREVENT Duty guidance (2015)

Rules for the Use of University Computer Equipment (*UoB-ISP2.03, UoB-ISP2.04*)

1. You must not remove computer equipment from the University without permission from an appropriate University Senior Manager.
2. You must not install unlicensed software or applications on University of Bolton computers, servers, laptops or mobile devices (UoB-ISP2.04)
3. You must not circumvent any security measures put in place to ensure the safe operation of computing equipment, information systems or communications equipment e.g. disabling anti-virus software, removing password protections etc
4. You must not install or use any device or software on University IT equipment that subverts or bypasses security controls including monitoring and filtering.
5. You must adhere to the terms and conditions of all license agreements relating to any software installed on, or accessed by, University computers including restrictions for commercial use.

Acceptable Use Policy for Students

University of Bolton

UoB-ISP3a



6. You may only access, modify, save or copy records or files and computer records where you have been given the authority and authorisation to do so
7. You must not create, access, transmit or download inappropriate or extremist materials, as defined within the Prevent Guidance (2015), using the University's IT systems or network. The University has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.
8. You must comply with the JANET network Acceptable Use Policy when using an internet connection from or to the University including, but not limited to, the following examples:
 - Not engaging in harassing, defaming or other anti-social behaviours on-line
 - Not creating or transmitting any offensive, obscene or indecent images, data or other material in any form
 - Not using the network to attack or gain unauthorised access to other network, computer systems or data
 - Not transmitting unsolicited bulk email (spam)
 - Not infringing the copyright of another person or organisation
9. You must ensure that you log out of University systems at the end of each session
10. You must not leave open-access computers "screen locked" for more than 20 minutes, thereby preventing others from using the shared resource.

Passwords, ID and Access (UoB-ISP2.03, UoB-ISP2.04)

Your unique User Identification code (User ID) and password are the primary control for access to the University's information systems, computer services and network. All access and activity that is logged can be tracked back to your user ID. Your User ID and password are for your sole use, therefore:

11. You must not use another person's user ID, nor permit or allow another person to use your user ID for any reason (UoB-ISP2.04)
12. Your password must be kept confidential. You must not allow your password to become known by another person. Disclosing your password to someone unauthorised in order to gain access to an information system or computer service may be a disciplinary offence (UoB-ISP2.03)
13. You must follow good security practices when selecting, using and protecting your passwords (UoB-ISP2.04) (UoB-ISP2.03)
14. The IT helpdesk service can reset your password if required. We will never ask you to divulge your password – beware of emails, and phishing phone calls that ask you to

disclose your password.

15. The University Internet Security Policy sets out the filtering and monitor policy. All Internet traffic passing through the University network, including email, is traceable through logs and is retained for set periods of time.
16. You must obtain explicit written and specific clearance from the University's Research Ethics Committee before engaging in research with materials on-line that are: highly controversial; sensitive; could expose you to harm or undue attention; or potentially breach University policies. For example political extremist sites, pornographic material, criminal activity or activity which is likely to give rise to civil action against the University.
17. The University has a statutory duty to co-operate with Law Enforcement Agencies in the course of an investigation, allowing access to your email, file spaces and any logged information, where a warrant/request is properly executed in relation to an investigation.

Protection against malicious code (UoB-ISP2.04)

Viruses, spyware, hacking utilities etc are classed as malicious code and are a risk to maintaining information security, therefore:

18. You must not deliberately, or through lack of care, allow malicious code or any other "nuisance" program or file onto any University systems. You must take the utmost care when downloading files from the internet or opening files attached to electronic mail (UoB-ISP2.04)
19. You must ensure that any non-University equipment you use to access University systems is free of malicious code e.g. with an up to date anti-virus product
20. You must not deliberately circumvent any precautions taken to prevent malicious code accessing University systems e.g. by disabling antivirus software
21. You must take steps to secure your computer when leaving it for a few minutes to avoid the risk of interference or misuse e.g. by locking the screen (UoB-ISP2.04)

Use of email and other electronic communication systems (UoB-ISP2.02)

22. The University and staff will correspond with by email using your bolton.ac.uk email address, regarding your study or on University business. You must check your University email regularly.
23. You must use your bolton.ac.uk email address when communicating with the University and staff so that your correspondence can be verified and tracked. Staff may not respond to email from other email domains because of the difficulty of establishing authenticity.

Acceptable Use Policy for Students

University of Bolton

UoB-ISP3a



24. You should not give serious attention to unsolicited email until and unless the sender's identity and authenticity of the mail have been verified (*UoB-ISP2.02*)
25. When attaching data files to an email that contain personal data i.e. data relating to living persons, e.g. for the purposes of research activity, the attachment must be encrypted to the University standard (AES256)

Use of Mobile devices (*UoB-ISP2.09a*)

26. You must take additional care when using mobile technologies to hold University data (including email) or access systems. You must adhere to the additional controls and requirements set out in the *Guide to Information Security for Mobile Devices*

Leaving the University (*UoB.ISP1.05*)

27. When you leave the University, or suspend your study, your computer user account will normally be suspended.
28. You must make all efforts to transfer important files from your University file space before you leave the University.

Disciplinary Process (*UoB-ISP2.03*)

29. Use and Access to University resources and information is conditional upon adherence to the Acceptable Use Policy. Where there is found to have been a deliberate attempt at unauthorised access, or wilful neglect to protect the University information systems and data, the University will initiate the appropriate disciplinary processes.
30. In the event that you breach the terms within the Acceptable Use Policy, your access to your user account may be suspended in order to allow an investigation to take place.

| This Policy to be Read by: | |
|-------------------------------------------|---|
| Staff | ✓ |
| Students | ✓ |
| Governors | |
| Consultants | |
| Partner staff of the University of Bolton | ✓ |
| Contractors of the University | |