Acceptable Use Policy

Purpose

This summarizes the key responsibilities and required behaviour of ***all*** users of the University of Bolton computer and information systems. The document should be read in conjunction with the University's Data Protection Policy and Information Security Policy which elaborates on the supporting policies, controls and rationale behind these requirements.

Policy

All staff, partner staff and contractors, and Governors 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.
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 not connect equipment to the University's *wired* network without permission from the Head of IST&L (UoB-ISP2.03)
9. You must comply with the JANET network Acceptable Use Policy when using an internet connection from or to the University including:
    - 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
10. You must ensure that you log out of University systems at the end of each session

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 but will never ask you to divulge 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 left unattended 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. Staff must only use University email for business purposes, in a way which is consistent with other forms of business communication *(UoB-ISP2.02)*
23. Staff must use their bolton.ac.uk email address when conducting email correspondence in relation to University business

24. Students must use their bolton.ac.uk email address when communicating with the University and staff so that correspondence can be verified
25. All email and electronic messages sent or received by staff that relate to University business, must be treated as being discoverable under the Freedom of Information Act or the Data Protection Act
26. 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)*
27. When attaching data files that contain confidential, sensitive or personal data to an email, the attachment must be encrypted to the University standard

Information handling *(UoB-ISP2.02, UoB-ISP2.04)*

28. All University Information can be classified according to its sensitivity as:
    - highly sensitive or confidential
    - sensitive
    - personal
    - internal (to the University) usage
    - public domain or unclassified

    Description and examples of these classifications are attached in Appendix A
29. When you create, access, copy or delete information, you must take into account its classification or likely classification and take all necessary steps to protect its confidentiality, integrity and availability. (UoB-ISP2.04)
30. You must not remove from the University, copy or share any confidential, sensitive or personal information either printed or held on computer systems without the proper authorisation of the information owner/custodian(UoB-ISP2.02)
31. You should only store, transfer or copy confidential/ highly sensitive, sensitive or personal information when the confidentiality and integrity of the data can be reasonably assured throughout the process, including those processes that involve partner organisations. (UoB-ISP2.02)
32. You must not use email to communicate confidential or sensitive or personal information unless you are sure that it is correctly addressed, secured appropriately and that the recipients are authorised to receive it. (UoB-ISP2.04)
33. You must make sure you have a back-up copy of any essential data that you create. Files on the University M: and L: drives are backed up each night. (UoB-ISP2.04)
34. You must take steps to protect confidential, sensitive or personal information from being viewed by unauthorised persons by:
    - only accessing from equipment in secure locations (UoB-ISP2.04)
    - Positioning the computer screens to avoid being overseen in public spaces
    - Using a locking screen saver when away from your computer

- Securely filing paper documents and shredding documents that are no longer needed. (UoB-ISP2.02.02)
- Closing down computers at night
- Clearing your desk of sensitive documents at night
- Not leaving printed documents unguarded on printers or photocopiers (UoB-ISP2.04)

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

35. 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)*

36. When you leave or cease to work for the University, you must return all information assets and equipment belonging to the University of Bolton, including computers, mobile phones, personal identification devices, access cards, keys, passes
37. Your access privileges will normally be removed immediately following your last contractual day. Part time and partner staff access can be renewed annually (UoB.ISP1.05)
38. Your emails and file spaces will be retained and archived for 4 years after you leave (7 years for key staff) (UoB.ISP1.05)
39. The University maintains the right to reallocate access to your University file store, workspaces and email. (UoB.ISP1.05)

Disciplinary Process *(UoB-ISP2.03)*

40. 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.

Appendix A Data Classifications

Unclassified / Public domain	Information which is not confidential or personal and which may be disseminated within the organisation and without. An example is the Prospectus
Internal	Data which is concerned with the running of the University prior to it becoming public domain. Examples include Committee papers.
Personal	Data which enables an individual to be identified; data which relates to or is about an identifiable individual. Such data may be processed lawfully by the University provided that staff comply with the DPA and the University's notification.
Sensitive	Personal data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs or other beliefs of a similar nature, (d) whether they is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992), (e) their physical or mental health or condition, (f) their sexual life, (g) the commission or alleged commission by them of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. Such data may be processed lawfully by the University provided that staff comply with the DPA and the University's notification
Confidential / highly sensitive	Data which may or may not be personal and which should not be disclosed, except to those to whom the information custodian sees fit and gives authority. Examples might be the University's application statistics, draft examination papers, financial information or a set of anonymised student mark profiles prepared for an assessment board.

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