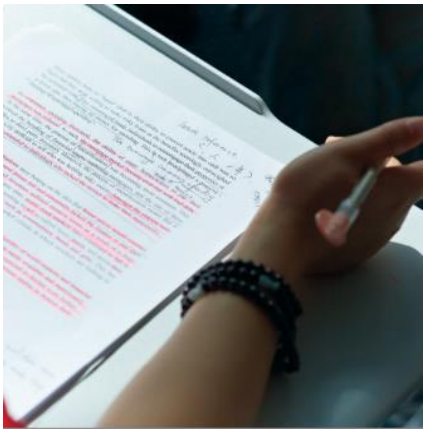
UNIVERSITY of BRADFORD

IT Services

Acceptable Use Policy



UNIVERSITY of BRADFORD

Version control

Approved by:	Executive Board (withdrawal of Regulation 21 approved by Council 6 July 2022)
Date approved:	5 July 2022
Next review date:	1 July 2025
Version number:	1.0
Applicable statutory, legal, or national best practice requirements:	ISO 27001:2013 Information Security Management Standard Computer Misuse Act 1990 UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Freedom of Information Act 2000

This document can only be considered valid when viewed via the University website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on the University website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

UNIVERSITY of BRADFORD

Contents:

1. Introduction

1.1 The University of Bradford relies on its information technology (IT) resources to enable its research, teaching and administrative activities. These resources are provided for legitimate and authorised purposes to serve the interests of the University.

1.2 The Acceptable Use Policy (AUP) provides a set of rules for using University IT resources and protects the University, users, and University property. It is the responsibility of every IT resource user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

2.1 The purpose of this policy is to outline the acceptable use of IT resources at the University of Bradford (the University). These rules are in place to protect all users and the University's IT systems and infrastructure, data, and intellectual property. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, fines, and legal proceedings.

2.2 An effective Acceptable Use Policy also ensures that authorised personnel have access to the information they need in a timely manner, ensuring the effective operation of the University.

3. Scope

3.1 This policy applies to students, employees, temporary workers, associates, visiting academics and other workers at the University, including all personnel affiliated with third parties such as contractors and consultants (users) and emeritus users. All users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and IT resource in accordance with the University's policies, standards, and applicable laws and regulations.

3.2 These resources include, but are not restricted to:

- Network infrastructure, including the physical infrastructure whether cabled or wireless, together with network servers, firewalls, connections, switches, and routers.
- Network services, including internet access, web services, email, wireless, messaging, file stores / drives, printing,

telephony and fax services, CCTV, and door and car park access control.

- IT infrastructure which includes University owned or leased computing hardware, both fixed and portable, personal computers, workstations, laptops, tablets, mobile devices, smartphones, identity tokens, servers, printers, scanners, disc drives, monitors, microphones, keyboards, and pointing devices. Network infrastructure and services, data centres, facilities and related equipment used to develop, test, operate, monitor, manage and / or support IT services thereby ensuring the reliable, efficient, and secure delivery of IT services.
- Software and databases, including applications and information systems such as Microsoft 365, virtual learning and video conferencing environments, IT laboratories, software tools, information services, data sets, citation databases, electronic journals, and e-books. It also includes software where the University has arranged commercial terms for students on commercial application packages.
- Online services arranged by the University, such as Office 365, JSTOR, or any of the JISC online resources.
- IT credentials, such as the use of the University login (username and passwords), or any other authentication method (email address, smartcard, dongle) issued by the University to identify users when using IT facilities. For example, users may be able to use drop-in facilities or Wi-Fi connectivity at other institutions using their University of Bradford username and password through the eduroam system. While doing so, they are subject to these regulations, as well as the regulations of the institution they are visiting.
- Electronic resources (e-resources) - materials in digital format accessible electronically, including, but not restricted to electronic journals (e-journals), electronic books (e- books), and online databases in varied digital formats.

4. Applicable laws and regulations

4.1 Users are bound by the laws of England and Wales when using the University's IT resources.

4.2 In addition, when accessing services from another jurisdiction, users must abide by all relevant local laws, as well as those applicable to the location of the service if different to the above. It is the user's responsibility to ensure their activities comply with these laws.

4.3 The use of the University IT resources is subject to all relevant University regulations.

4.4 When making use of the internet, the acceptable use policies of the carriers apply, in particular, the Joint Academic Network (JANET). An overview of laws relating to the use of IT resource can be found on this website: https://www.jisc.ac.uk/guides/networking-computers-and-the-law

4.5 Any information you create or store on University systems is subject to the Freedom of Information Act 2000, and the Environmental Information Regulations 2004, and may be disclosed in response to a request made under these laws.

4.6 Users must use all appropriate means to ensure that personal data is protected in accordance with Data Protection legislation.

4.7 Furthermore, all data processed on University systems are subject to UK Data Protection Legislation, i.e., the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. This means that the personal data of others must be processed lawfully and fairly and again may be disclosed in response to a request made under these laws.

4.8 All use of University IT resource is covered by the Computer Misuse Act 1990 which prevents unauthorised access to computer for the purposes of committing or facilitating the commission of further offences. Attempting to use IT resource without the University's permission may constitute a criminal offence under the Act.

4.9 All use of IT resource and e-resources is covered by the Copyright Designs and Patents Act 1988 which prevents the copying of material whose copyright is owned by other people.

4.10 Users must comply with all relevant copyright legislation, licences and agreements for software and e-resources when accessing and connecting to University IT resources and must obtain authorisation from IT Services for purchasing / obtaining software and software licences, and for installing such software on University owned computers.

5. General use and ownership

5.1 IT resources are provided to users primarily for University business to support teaching, learning, research and innovation, and professional and administrative services.

5.2 Only authorised users of the University's IT resources are permitted to use them. If you have any doubts as to whether you have the authority to use an IT resource, you should seek further advice from IT Services.

5.3 Users may access, use, or share the University's proprietary information only to the extent it is authorised and necessary to fulfil their assigned job duties.

5.4 The theft, loss, or unauthorised disclosure of University equipment or data must be reported promptly.

5.5 The University may monitor equipment, systems, usage, and network traffic etc. at any time for security and network maintenance purposes, preventing or detecting criminal activities, and to ensure compliance with University Regulations and Policies. The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.6 All users should be courteous and considerate of others when using IT resources. The use of social media should be done with discretion and not abused.

5.7 The IT account of a member of staff may need to be accessed during their absence. Any such access will only be granted in accordance with any procedure covering this process.

5.8 USB memory sticks should not be used for personal, confidential, or sensitive data unless encrypted.

5.9 The University only endorses and supports the use of cloud computing services for the management and storage of University information where the service has been approved for use by IT Services. In the absence of an approval, such systems should not be used.

5.10 Users should take reasonable precautions to ensure that information is not transmitted to the wrong person; check that outgoing emails are addressed to the correct recipient before sending emails.

5.11 Users should take reasonable measures to ensure the prevention of loss or theft of University IT equipment. University IT equipment should not be left unattended in cars or in public areas or while travelling. University IT equipment should be kept securely when not in use.

5.12 Occasional and limited personal use is permitted, provided this is compatible with, and does not contravene, the primary purpose of the IT resource. Users are responsible for exercising good judgment regarding the reasonableness of this personal use: if there is any uncertainty, contact IT Services, your manager, or course leader in the case of students.

6. Security

6.1 Each user is issued with a valid username and password which must be used to authenticate and gain access to the IT resources. All users are responsible for all activity that takes place under their username and must not allow anyone else to access the IT resources using their username and password. Access to the IT resources using someone else's username and password is prohibited. Sharing of passwords is strictly forbidden.

6.2 All passwords, both system level and user passwords, must comply with the Password Policy.

6.3 Users must exercise good information security and management practices for the storage, access, retention, and deletion of University information.

6.4 All mobile devices that connect to the University internal network must comply with the Mobile Device Policy.

6.5 All computing devices must be secured with a password-protected screensaver.

6.6 Computers must be locked or logged off when the device is unattended, this will not be applicable when a computer is carrying out rendering jobs e.g., printing.

6.7 All personal devices used to access UoB resources should be password protected with at least 4 characters.

6.8 Users must use extreme caution when opening email attachments, these may contain malware.

7. Unacceptable use

7.1 The following activities are strictly prohibited. This list is not intended to be exhaustive but provides a framework for activities which fall into the category of unacceptable use.

i. Causing the good name and or reputation of the University or any part of it to be damaged or undermined by carrying out or facilitating criminal, inappropriate, or other activity that conflicts with any relevant law of the values, charter, statutes, regulations, or policies of the University.

ii. Violating the rights of any person, the University assets protected by copyright, trade secret, patent, or other intellectual property, or laws or regulations, including, but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by the University.

iii. Unauthorized replication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the University or the end user does not have an active license, is strictly prohibited.

iv. Accessing data, a service or server, or an account for any purpose other than conducting the University's business, even if you have authorised access. Introduction of malicious programs such as viruses, spyware etc. into the University's network, or using it to transfer such programs to another network.

v. Making fraudulent offers of services or items originating from any University account.

vi. Accessing or seeking to access restricted areas of the University's network e.g., Server rooms, wring closets etc.

vii. Circumventing user authentication or security of any computers and phones, network, or account.

viii. Executing any form of network monitoring which will intercept data not intended for the user's host unless this activity is a part of the user's normal job / duty.

ix. Crypto Currency mining.

x. Port scanning, or security scanning.

xi. Introducing honeypots, honeynets, or similar technology on the University's network.

xii. Using any program / script / command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network session, via any means, locally or via the internet / intranet / extranet.

xiii. Providing the personal data of University staff or students to third parties without authorisation.

xiv. Sending unsolicited email messages, including the sending of 'junk mail' or other advertising material to individuals who did not specifically request such material (email spam).

xv. Any form of harassment via any form of communication means, whether through language, frequency, or size of messages.

xvi. Unauthorised use, or forging, of email header information.

xvii. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

xviii. Creating or forwarding 'chain letters', 'Ponzi' or other 'pyramid' schemes of any type.

xix. Use of unsolicited email originating from within the University's networks or other internet / intranet / extranet service providers on behalf of, or to advertise, any service hosted by the University or connected via the University's network.

xx. Posting excessive numbers of non-business-related messages to large numbers of users. This may lead to a distributed denial of service (DDOS); where a website exceeds its capacity to handle multiple requests.

xxi. Carrying out personal or non-University commercial business e.g., gambling, sales, advertisements etc.

xxii. Carrying out activities that conflict with a member of staff's obligations to the University as their employer, including selling any part of the IT resources and carrying out activities of a nature that competes with the University in business.

xxiii. Deliberately or unintentionally, access, create, change, store, download, upload, share, use or transmit:

a) any terrorist related or extremist material (other than during properly supervised, lawful, and authorised research) in accordance with the Prevent Duty imposed by the Counterterrorism and Security Act 2015.

b) any illegal, obscene, or indecent images, data, or similar material (other than during properly supervised, lawful, and authorised research).

c) any infected material or malicious code (including, but not restricted to, computer viruses, spyware, trojan horses and worms) whether designed specifically or not to be destructive to the correct functioning of computer systems, software, networks, data storage and others' data, or attempt to circumvent any precautions taken or prescribed to prevent such damage.

d) any material which discriminates or encourages discrimination on any grounds.

e) any material which the University may deem to be advocating, inciting, or encouraging illegal activity; threatening, harassing, defamatory, bullying or disparaging of others; abusive, libelous, slanderous, indecent, obscene, offensive, or otherwise; causing annoyance, inconvenience, or needless anxiety.

7.2 The following are exemptions to this section:

i. Authorised internal and third-party Security testing is exempt (7 iv)

ii. Authorised security testing is exempted (7 xi)

iii. Hacking / cyber security courses and authorised research work and use are exempt.

8. Exit from the University

8.1 Upon leaving the University, users must abide by the following:

i. Ensure any personal information they wish to retain is transferred from the University's systems, as access will be denied and, in time, deleted as per the University's Records Retention Schedule.

ii. Ensure any data which belongs to the University is not deleted.

iii. Ensure any data which may be needed by the University is transferred to an appropriate location, or to an appropriate colleague prior to departure.

iv. Ensure University information is removed from personal devices.

v. Ensure any data which may be needed by the University is not deleted and is transferred to an appropriate location, or to an appropriate colleague prior to departure.

vi. Ensure conformity with any other procedures set out by the University in relation to departure.

vii. A mandatory return of all University owned device is required before exit.

8.2 Line managers must ensure that the above steps are taken prior to a member of staff's departure from the University, and provide advice on this, where necessary.

9. Exceptions

9.1 Where, for operational reasons, staff may be exempted from these restrictions during their legitimate job responsibilities, any such exception must be requested in accordance with any published process and approved by HR and the Director or Associate Director of IT Services.

10. Policy compliance

10.1 The University IT Services team will verify compliance to this policy through various methods including, but not limited to, business tool reports, internal and external audits, and feedback to IT Services.

11. Infringement

11.1 Breach of this policy will be handled by the University's Student and Staff Disciplinary Procedures. These include a range of sanctions up to and including expulsion from the University / termination of employment.

11.2 In cases where an alleged breach has been undertaken by someone who is neither a member of staff nor a student, an investigation

will be conducted by a senior Manager of IT Services in conjunction with University Secretary or their nominee.

11.3 Breach by a third party may lead to termination of contract and claim for damages.

11.4 Where an offence has occurred under applicable law, it may also be reported to the police or other appropriate authority and could lead to civil or criminal proceeding.

11.5 The breach of this policy may potentially result in the suspension or removal of university IT facilities or equipment.

11.6 Users who require any assistance with interpreting or applying this policy should contact IT Services on +44 (0) 1274 233333.

12. Related policies and standards

This policy forms part of the Information Security Policy Framework and should be read in conjunction with the policies, regulations, standards, and procedures contained therein, in particular:

- All IT related policies
- Information Security Policy
- Data Protection Policy
- Freedom of Information Policy
- Records Retention Schedule
- Mobile Device Policy
- Student Disciplinary Procedure
- Staff Disciplinary Procedure
- JISC System Administrators' Charter

13. Monitoring and review

This policy will be reviewed next in March 2025, or as appropriate, and in response to changes to legislation or University policies, technology, increased risks, and new vulnerabilities, or in response to security incidents.