Acceptable Use Policy (AUP) - Summary Overview

This summary overview highlights the key aspects in the Acceptable Use Policy (AUP) for all ICT (Information Communication Technology) Resources and Network Users. The AUP is a combination of a number of key documents which indicates and promotes the appropriate use of ICT resources, data, information, networking and systems in the interest of learning, teaching, research, administration and management.

Key Points:

1. Using AUB ICT resources and networking means agreeing to abide by the Acceptable Use Policy.
2. Data and information that users maintain must be accurate, timely, and secure and any actions of the user must take responsibility for control and maintenance of that data inline with GDPR.
3. All University data must be stored on university approved systems. This includes student data, but also intellectual property, financial data, and materials generated in electronic format by a user in the employment of the university. No data may be transferred to external systems (for example personal drives, YouTube, online data analysis systems, such as AI) without permission and a data risk assessment.
4. Use of AUB ICT resources and networking must not interfere with other users or the integrity of AUB systems.
5. Users are not permitted to use the University's network to support, promote or promulgate any information which may be considered contrary to the University's Prevent Policy, or its Safeguarding Policy. Accessing material which is obscene or abusive may be illegal and may also be classed as harassment and contravenes this policy.
6. All users must have their own username and password and not use anyone else's account for any purpose without expressed consent.
7. AUB licensed software can only be used for educational purposes as aligned with the third-party contract agreements within the express permissions of the end user licence. For example, these often prohibit the use of educational licenses for commercial purposes.
8. Users have the responsibility to ensure all information must remain 'fit for purpose' in terms of its accuracy, access and timely nature of its content, and must be appropriate for the business of the University.
9. Confidential or sensitive data should not be maintained on removable media or non AUB approved cloud-based storage, unless prior agreement has been arranged through the Head of Digital Services.
10. All credit card payments should be taken via Finance or via third party with Finances prior approval. No card details are to be recorded or stored outside of these approved provisions.
11. Email and online communications are regarded as official AUB communication regardless of content. All communications must be appropriate and professional.
12. Communication systems (email / telephone / messaging) may only be used when we have the owner's permission to maintain contacts details. These systems must only be used for business purposes as identified to the recipient when gaining prior approval.
13. All electronic communications fall under the Freedom of Information Act and GDPR. They can therefore fall under FIA Applications or Subject Access Request. AUB have the right to review email and communication systems without the user's consent following approval through the Director of People / Vice-Chancellors Office.
14. All users and mobile devices can join the 'Eduroam' wireless network provision with appropriate username and passwords. There are also Guest and Event provisions available.
15. Telephone calls are monitored for cost centre purposes and any personal calls should be as brief as possible.
16. Mobile Phones are available for external trips and for publishing of mobile contact details. At no point is it required to give student groups your personal contact details unless prior consent given.
17. Any failure to comply with the AUP may result in disciplinary action.

Acceptable Use Policy (AUP)

Introduction

1.1 The Acceptable Use Policy (AUP) indicates and promotes the appropriate use of ICT resources, data, information and systems in the interest of learning, teaching, research, administration and management.

1.2 This AUP is applicable to all computing and network facilities provided and supported by the Arts University Bournemouth (AUB) and those services supplied through the Joint Academic Network (JANET) provision.

1.3 Nothing in this Acceptable Use Policy should be read as undermining or conflicting with our Code of Practice on Freedom of Speech; and in the case of any conflict the Code of Practice will take precedence.

1.4 The use of data and information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as AUB, which has a formal duty to protect its data, information and systems to minimise any effects of inappropriate access, uses, breaches or security incidents.

1.5 This policy also indicates security processes for data and information held on the University's computers / servers / network and its use by established members of the University in their official capacities. It is vital that data remains accurate, timely, secure and confidential and any actions of the users show responsibility for control and maintenance of that data, especially with information systems becoming increasingly accessible online for wider accessibility.

1.6 All ICT resources and network access provided by AUB for use by staff, students, visitors and contractors are subject to the University's Acceptable Use Policy.

1.7 This policy is intended to safeguard the University, staff, students and owners of intellectual property rights from information security related incidents and any other consequential action.

2.0 Acceptable Use Policy

AUB ICT resources and networks are provided to facilitate access for staff, students, visitors and contractors specifically for educational, research, training and administrative purposes. Use of ICT resources and networking must not interfere with the users, or any other person's duties or studies.

2.1 All computer systems (staff and students) are restricted by account authentication through a username and complex password. Accounts are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. Any attempts to access or use any username not authorised to the user is prohibited and may result in disciplinary action. It is also a criminal offence to gain or attempt to gain unauthorised access to a computer system.

2.2 No-one may use, or attempt to use, computing equipment allocated to another person without the express consent of the individual involved. If a user is absent from work or their course, they can provide consent to provide specific access to their account If consent is not available and access is required as part of a formal investigation, then a written request must be authorised through the Head of Human Resources / Vice-Chancellors Office.

2.3 No person shall jeopardize the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the University's computer systems is put at risk if users do not take adequate precautions against cyber-attack or malicious software, such as computer viruses or malware. Any such breaches will be taken seriously and referred through the Vice-Chancellors Office.

2.4 Distributing or accessing material which is obscene or abusive may be illegal and may also be classed as harassment and contravenes this policy. If a user needs to access material which may be considered obscene or abusive as part of legitimate University business, they must first secure approval from the Head of Digital Services, who will consult with colleagues as required.

2.5 Unsolicited advertising or 'spamming' is not acceptable and may also be considered harassment.

2.6 Users are not permitted to use the University's network to support, promote or promulgate any information which may be considered contrary to the University's Prevent Policy, or its Safeguarding Policy. Any material which contravenes this will be deemed a *prima facie* breach of the Acceptable Use Policy. The University systems are protected by firewalls, and JANET monitoring. Any member of staff or student who may require access to sensitive or terrorism-related material for academic purposes should contact the Head of Digital Services prior to accessing it from the University network to ensure that this access is properly authorised.

2.7 Any information and/or hard copies of data which is not generated by the user personally and which may become available through the use of AUB computing or communications services, shall not be copied or used without permission of AUB or the copyright owner.

2.8 Software provided by the University may only be used as part of the users' duties as an employee or student of AUB or for educational purposes. The user agrees to abide by all the licensing agreements for software entered into by AUB with third parties.

3.0 Information Security

3.1 The University recognises the role of data and information security in ensuring that users have access to the information they require to carry out their work. Computer and information systems underpin all the University's activities, and are essential to its learning, teaching, research and administrative functions.

3.2 The University is committed to protecting and ensuring the security of its data / information and information systems to ensure that:

1. the integrity of information is maintained so that it is accurate, up to date and 'fit for purpose'
2. information is always available to those who need it and there is no disruption to the business of the University
3. confidentiality is not breached, so that information is accessed only by those authorised to do so
4. the University meets its legal requirements, including those applicable to personal data under the Data Protection Act and General Data Protection Regulation (GDPR).
5. the reputation of the University is safeguarded

3.3 The University is also governed by PCI-DSS (Payment Card Industry Data Security Standards) in the way it handles credit card payments to ensure appropriate controls are in place for taking and maintaining credit card details. All card payments should be taken through Finance and Online Store with no need to record or store any card details outside these provisions.

4.0 Principles

4.1 The Computer Misuse Act 1990 applies to everyone who uses a computer. It is a criminal offence to seek unauthorised access to any computer or computer system, or to make an unauthorised modification to any computer material. Therefore staff and students should not use any computer equipment without permission and should not try to access information unless authorised to do so.

4.2 A computer password provides access to computer resources and associated data. It is the employee's personal responsibility to keep passwords secret and ensure that they are changed regularly.

4.3 When using ICT resources (computers, mobile and storage devices) it is essential for employees to protect themselves against the loss of important data and information. This is through maintaining currency on files and ensuring any sensitive data and information is appropriately maintained within AUB management information systems. Appropriate data should be maintained and backed up only on AUB systems.

4.4 Confidential and sensitive data should not be maintained on USB memory sticks, portable hard drives, non AUB email systems or cloud based storage provision in the normal business operations of AUB. If the case arises, these files should be password protected / encrypted and deleted once work is completed and returned onto AUB systems. If this process is not followed and sensitive data is lost, this will result in disciplinary actions.

4.5 All staff with access to information have a responsibility to handle it appropriately according to its classification and to maintain confidentiality and integrity. Users having privileged/guardian access and/or systems update rights may not use such privileges for; personal gain, deception, fraud, use of unauthorised software or for any other purpose other than University business. Nominated staff are responsible for ensuring that appropriate procedures, systems and security measures for the processing and holding of information are in place and are effective.

4.6 The Data Protection Act imposes statutory conditions for the maintenance of personal data on the University computer systems including data held by individual members of staff on their individual computers. All personal data should be kept secure. It is an offence to use or disclose such data if not registered to do so under the Data Protection Act.

4.7 GDPR maintains the process activities and control for personal and sensitive data held within AUB and ensures the legal liability and responsible for any data breach. Training is maintained to ensure data controllers and processors are up to date with GDPR legislation.

4.8 Under the Copyright, Designs and Patents Act 1988 computer software is protected and under no circumstances may copies or 'pirated' versions of software be held or used as this amounts to infringement of copyright and the University could be sued for damages.

5.0 **Responsibilities**

5.1 All University information systems are subject to potential loss of data due to failure of hardware or software. It is the responsibility of Digital Services in the case of centralised systems and users for local systems to ensure that regular backup copies of essential data are made and stored in safe locations (on premise and hosted). If there is a risk that the entire system may be lost as a result of a disaster e.g. fire or flood, the AUBs Business Continuity Plan (BCP) is in place to ensure academic and business continuity.

5.2 Digital Services is responsible for ensuring that all computer systems are effectively managed to ensure information confidentiality, integrity and availability. This includes ensuring proper user administration (access controls, security mechanisms) and data administration (permission access, security mechanisms, vulnerability testing, backup, archiving and safe hardware disposal etc.) as well centralised approval and purchasing of all AUB software and hardware.

5.3 The University recognises that compliance with this policy cannot be achieved without the active support of its employees. Managers should ensure that all employees are aware of their responsibilities. These responsibilities include:

- understand to which information and data they have a right of access
- know the information for which they are guardians
- know the systems and hardware for which they are utilising.
- be aware of this policy and comply with it

5.4 Compliance with this policy will be enforced. Breaches of information security controls must be reported to the University Secretary and Compliance Officer acting as the Information Controllers to enable a full University Management Team review.

5.5 Relevant legislation includes, but is not limited to:

- The Computer Misuse Act (1990)
- The Data Protection Act (2018)
- General Data Protection Regulation (2018)
- The Regulation of Investigatory Powers Act (2000)
- The Freedom of Information Act (2000)

6.0 Users and External Parties

6.1 Users of University ICT and data will be made aware of their own individual responsibilities for complying with the University policies on ICT resources and information security through IT Inductions, GDPR training and line management processes.

6.2 Agreements with third parties involving accessing, processing, communicating or managing the University's information or information systems, should cover all relevant security requirements and be specifically mentioned in contractual arrangements.

6.3 Compliance with this policy should form part of any contract with a third party that may involve access to AUB network or computer systems or data.

7.0 Storage Devices

7.1 The use of USB memory sticks, portable hard drives, mobile devices and approved cloud storage provisions are allowed for the movement of large media data files which are often created in the University (images and media content).

7.2 Copying or emailing of sensitive data / information which contains any student or staff information to any device or cloud provision is prohibited, unless specifically approved. If the requirement exists then firstly this must be discussed with Digital Services to try and identify a more appropriate option, if no other option exists, then authorisation must be made through your line manager and the file password protected / encrypted so if lost or stolen the contents could not be read. Passwords to encrypted data should never be shared using the same method as the data itself. If this process is not followed and sensitive data is lost this may result in in disciplinary action.

7.3 Staff remote access to AUBs core information systems (Student Records; Finance & HR) is supported through a secure Citrix virtual desktop infrastructure. This provides a remote computing arrangement for staff to access core systems from any location through a permissioned service.

Personal and Sensitive data or confidential files should not be maintained on laptops or mobile devices without being password protected or encrypted. All files should be stored appropriately on AUB fileservers or within the AUB Microsoft365 tenancy, such as OneDrive.

8.0 Passwords

8.1 AUB utilises 'complex' password authentication to protect computer, network resources and online services. 'Complex' passwords are now standard practice with the use of a minimum 8 characters with a mixture of numbers and case sensitive letters.

8.2 The use of 'complex' passwords is utilised to offer permission based access to systems, data and information and to extend the range of University services and resources online.

8.3 Staff and core system passwords are changed every 90 days to ensure data and systems are securely maintained and minimise any unauthorised breaches. Students are required to change their 'complex' password at the start of each academic year.

8.4 Passwords will only be reset via the Digital Services ServiceDesk once identification of the user has been verified through recognition or AUB ID card. In the rare occurrence of a remote worker (such as a Visiting Tutor) requiring a password reset, this will be done by confirming information with the user and their line managers authorisation.

8.5 Passwords should never be written down, stored online, emailed, shared or disclosed. Users should ensure their computer is locked or logged out whenever they leave their desk.

9.0 Email

9.1 AUB email is hosted through Microsoft Office 365 for Staff and Students. Mailboxes are limited in size to 100gb and have a maximum limitation of a 10,000 email transactions per day.

9.2 An email attachment limit of 50MB is utilised within AUB. It is recommended that files are not sent via email, rather uploaded to OneDrive and shared from there. This is a more secure method and allows for the sharing of files over 50MB. It's vital that users manage who has access to their files, always keeping access to a bare minimum. Assistance can be requested through Digital Services in this regard.

9.3 All staff and students have individual mailboxes for which only the named person can access using their username and password. At no point should others have the ability to review individual mailboxes without the expressed consent of the individual involved.

9.4 Whilst it is appreciated that AUB email is mainly communication on matters directly concerned with the business of the University, the content should still be regarded as private and confidential to that individual.

9.5 In regard to absence through an extended period of time and the need to access that users mailbox, this must, in the first hand, be with the individual's direct consent. If consent is not available or email audit is part of a formal investigation, then written request must be authorised through the Head of Human Resources / Deputy Vice-Chancellors Office.

9.6 Staff should actively manage their mailbox accounts (Inbox, Sent, Deleted) to ensure no sensitive or confidential emails remain when no longer required. Users should maintain good housekeeping skills and ensure that emails are deleted and only relevant and timely correspondence is maintained.

9.7 Email Virus, SPAM and Anti Threat Protection operate to define and quarantine malicious or inappropriate emails. Workflows exist to automatically delete or provide an overview area for users to review and allow / reject mail content. These systems are based on external dictionary based triggers which are constantly update through third party security and virus vendors.

9.8 Distribution groups are specifically created for various staff and students groups. Restrictions are in place to prevent unauthorised sending to 'all staff' and 'all students' in which only certain named staff are able. Clear messages will be displayed if your email to groups is undeliverable.

9.9 AUB email communications are regarded as official university communication regardless of content and could possibly expose the user and AUB to unnecessary risks. Please take care when sending emails as contents can be regarded as contractual and raise elements for legal claims, including libel and breach of contracts.

9.10 All email communication must be appropriate and professional and not cause unnecessary misunderstanding or distress. Emails can be used as an audit trail, for example in disputes or investigations. .

9.11 AUB have the right to review mailboxes without the user's consent following approval through the Head of Human Resources / Deputy Vice-Chancellors Office.

10.0 SMS (Texting) – Small Message Service

10.1 AUB utilises an integrated SMS service through a number of its management information systems (SITS, Finance and Student Advice) which are used against specific tasks with individuals' prior agreement to hold a mobile contact number and to contact in this manner.

10.2 SMS is also used for specific course communication for which instant communication is appropriate such as Saturday Arts School (under 16) and Evening Courses, specifically for class cancellations and parent communication.

10.3 The hosted SMS service also supports staff communication mainly in respect to business continuity (snow days) and major incident situations. Staff are informed of this provision when contractually joining AUB for the specific use of contact in these situations.

10.4 These systems are not widely available and are only used for agreed communication / escalation tasks. The Director of Finance & Planning controls management overview of the SMS service.

11.0 myAUB

11.1 AUB uses myAUB as its authenticated portal gateway for students and staff to access AUB online resources and services. This includes access to email, calendars, timetables, learning environments, information including documents and additional reference presented securely within the AUB Intranet.

11.2 myAUB is accessed by your username and password which then personalises parts of the portal content to the individual user, group or section depending on the users inherited permissions. The content of myAUB therefore offers secure authorised access to some specific information, documents and management reports relevant to the user. Username and passwords must be kept confidential and not given to any other third parties.

12.0 Bring Your Own Device (BYOD)

12.1 Staff are supported in utilising mobile AUB owned computing devices (laptops) through the 'AUBCOBO' wireless network service which is joined through username and password authentication and gives full access to the AUB computer network. COBO – Company Owned, Business Only.

12.2 AUB supports students and staff in utilising personal mobile computing devices (laptops, tablets, mobiles) through the 'EduRoam' wireless network service which is joined through username and password authentication and is available on campus and at a number of other education and government institutions. EduRoam – Educational Roaming.

12.3 AUB Guest WIFI is available for individuals or events and can be accessed via a code, please contact ServiceDesk for more information

12.4 Guest access and EduRoam only provides basic Internet access for web access and open AUB web services.

12.5 AUB owned mobile devices such as phones and tablets which have secure email connections and access to specific services, must be configured to AUB's mobile device management system and configured to use a 6-digit passcode or biometric challenge and ability to reset the device in the event of being lost or stolen.

12.6 Non AUB owned devices are not to be connected to the wired AUB network as they pose a cyber security risk to other users.

13.0 Telephones

13.1 All external telephone calls from AUB are monitored and registered for cost centre purposes and regularly reviewed. It is appreciated that most calls to students are via mobiles for which call charges are considerably higher than landlines.

13.2 It is not expected that staff will routinely make use of the University telephones for personal reasons. However, if individuals need to make personal calls it should be as brief as possible.

13.3 By default, all AUB phones are barred from making international calls unless specific permission has been obtained by the sections Director to remove the barring.

13.4 Staff must borrow a loan mobile phone for any trips or international duties so contact details may be published and direct contact can easily be maintained by AUB. At no point should staff give personal mobile contact details to students.

14.0 Enforcement

14.1 The Acceptable Use Policy (AUP) must be provided to every user and published online for easy reference so that they are aware of their responsibilities.

14.2 Any failure to comply with the policy may result in disciplinary action or, in relevant cases, criminal prosecution.

14.3 Any loss or unauthorised disclosure must be promptly reported to the owner of the information.

14.4 Computer security incidents involving the loss or unauthorised disclosure of personal data / information held in electronic form must be reported to the University Secretary and Compliance Officer immediately and investigated.

15.0 Other Relevant University Policies or Guidance

- JANET Acceptable Use Policy:
  https://community.ja.net/library/acceptable-use-policy
- Data Protection:
  https://intranet.aub.ac.uk/compliance/data-protection/
- Freedom of Information:
  https://intranet.aub.ac.uk/compliance/foi/
- Information Management:
  https://intranet.aub.ac.uk/compliance/information-management/
- Safeguarding Policies, including Prevent Policy

The Arts University Bournemouth is committed to the provision of a working and learning environment founded on dignity, respect and equity where unfair discrimination of any kind is treated with the utmost seriousness. It has developed and implemented a Single Equalities Scheme (SES) to guide its work in this area. All the University policies and practices are designed to meet the principles of dignity, respect and fairness, and take account of the commitments set out in the SES.