AECC University College

Version: 2.1
Effective From: 06/07/2021
Policy Owner: Head of IT

IT Acceptable Use Policy

1 Purpose and Scope

1.1 AECC University College makes extensive use of its IT facilities for its teaching, learning, research, administrative and managerial activities. The use of these facilities provides many benefits, opportunities and efficiencies to all functions of the University College, yet also introduces a number of risks and threats to the institution and its users. The use of these technologies therefore requires effective management in order to maximise the benefits and minimise the risks for the mutual benefit of all stakeholders.

1.2 Use of University College IT facilities constitutes acceptance of this policy. If you do not agree or understand any aspect of this policy you must logout, disconnect or stop using the IT facilities immediately. Please contact the IT team for clarification if required.

1.3 This policy applies to the use of all IT facilities & services provided by AECC University College or by third parties on behalf of AECC University College. These include, but are not limited to:

- ALL computers, irrespective of ownership when connected to the AECC University College network or IT facilities from ANY location (internally and remotely)
- Physical or virtual computers, servers and desktops
- Mobile devices, laptops, tablets and smart devices
- Peripherals such as monitors, keyboards, copiers and printers
- All wired and wireless networks
- Software and data on University College IT systems
- Computer based information systems provided for any purpose
- Virtual Learning Environments (i.e. Moodle)
- Email and other electronic communication systems
- Telephony systems
- All data storage systems
- External resources including Janet, Eduroam, ‘The Cloud’ and other or successor networks and systems
- External Cloud computing providers

2 Intended Audience

2.1 This policy applies to all individuals who have been granted access to any IT facilities and services provided by or through the University College. This includes, but is not limited to:

- All members of staff including temporary and agency staff
- All registered students including short course attendees
- Third parties i.e. contractors or sub-contractors engaged to undertake work for the University College
- Research students, PhD Students and Research fellows
- Remote radiologists and reporters
- External examiners
- Guest lecturers
- Any user of the public wifi service

3 Associated Policies

3.1 This policy is the core of a framework of policies, which must be considered as a whole to ensure effective operation of University College IT and associated resources and services:

- IT User Access Policy
- IT Security and Password Policy
- Data Protection Policy
- Remote Working Policy
- Bring Your Own Device (BYOD) Policy
- Patch Management Policy

The following University College policies and documents are also pertinent:

- Administrator's Code of Conduct
- Communications Policy
- Student Handbook
- Student Agreement
- Code of Conduct
- AECC University College Brand Guidelines
- Prevent Policy
- Copyright Policy
- Policy on the Provision and Use of Electronic Resources via the Virtual Learning Environment (VLE) and Recording of Lectures

4 Legal Responsibilities

4.1 This policy incorporates the acceptable use policy of AECC University College's service provider, JISC, which provides and manages the high speed Janet network for the UK research and education community. The full JISC acceptable use policy can be viewed here: https://community.jisc.ac.uk/library/acceptable-use-policy

4.2 In addition, the use of IT facilities within AECC University College is subject to applicable legislation and regulations governing the use of UK academic computing and communication facilities. The following list is not exhaustive, but includes the most notable legislation and regulatory items:

- Computer Misuse Act 1990 which defines activities such as hacking or the deliberate introduction of viruses a criminal offence
- Access to Health Records Act 1990
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- Equality Act 2010
- Prevent Duty / Counter Terrorism Security Act 2015
- The Data Protection Act 2018
- General Data Protection Regulation (GDPR) 2018

4.3 The University College has a statutory duty under the Counter Terrorism Security Act 2015 to have due regard to the need to prevent people being drawn into terrorism.

4.4 The University College has a responsibility to support freedom of speech and academic freedom but within the constraints of current legislation.

4.5 Users are responsible for complying with all agreements and terms and conditions while using IT resources including but not limited to:

- Software / Website license agreements and Terms & Conditions
- Copyright Agreements
- Acceptable Use Policies of any third party networks or services accessed through the University College's IT Facilities
- Relevant government, local telecommunications and networking laws and regulations

5 Violations

5.1 Actual or suspected violations should be reported to the Head of IT who will determine the correct actions to be taken. Users should not under any circumstances make attempts to perform investigations themselves.

5.2 Violations will be reviewed on a case-by-case basis and may result in access to University College IT facilities being denied (either temporarily or permanently) and, depending on the severity of the breach, disciplinary action including termination of employment or study at AECC University College. If it is believed that a criminal action has occurred, the relevant law enforcement agencies will be involved as necessary which may lead to court proceedings attracting both criminal and civil liability. The University College also reserves the right to advise third parties of any infringements of their rights, and to pursue civil damages against any party.

5.3 Where a serious breach of the data protection legislation has occurred i.e. where a substantial loss of, or unauthorised access to personal information has occurred (volume or sensitivity) then the University College Data Protection Officer (DPO) will assess whether the University College is required by law to notify the UK Information Commissioner's Office within the appropriate timescale.

6 Acceptable Use

6.1 The University College IT facilities are provided to staff and students for University College related teaching, learning, research, administrative and managerial activities.

6.2 Occasional and reasonable personal use is permitted, provided this does not interfere with the availability of University College IT facilities for non-personal use or the performance of learning or a member of staff's responsibilities. The University College considers acceptable personal use to include activities such as online shopping and banking. Purchases or other transactions made online however are made entirely at the user's own risk. University College email addresses must not be used to sign up for personal accounts or services or personal purchases and must only be used in connection with institutional business. Similarly, personal email addresses and accounts must not be used to conduct University College business.

6.3 Users may use IT facilities for personal improvement and learning, provided that such use is consistent with professional conduct and is not for personal financial gain or breaches of the law.

6.4 The University College does not provide any guarantees regarding the privacy or security of any personal use of University College IT facilities and users do so at their own risk. Any personal material and information stored on University College IT facilities can be accessed by the University College in the same way as it can access other material and information.

7 Unacceptable Use

7.1 Users must NOT use the University College IT facilities for any activity that may reasonably be regarded as unlawful, or potentially unlawful. This includes, but is not limited to, any of the following activities:

- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Adding or creating material that promotes or incites racial or religious hatred, terrorist activities or hate crime; or instructional information about illegal activities.
- Promoting, or perceived to promote, discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion or disability.
- Threatening, indecent, intimidating or violent behaviour.
- Any form of 'cyber bullying, harassment or victimisation'.
- Creation or transmission of material with the intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or the University College has chosen to subscribe.
- Gambling or personal financial gain.
- Misrepresenting personal views as those of the University College.
- Entering AECC University College into any contractual or financial commitment unless specifically authorised to do so.
- Dispersing institutional data without authorisation.
- Unauthorised disclosure of personal, confidential or sensitive information belonging to the University College, its employees, contractors, suppliers, employees or clients or any information which could be used by one or more of the University College's competitors, for example information about the University College's work, its products and services, technical developments and staff morale.
- Failure to ensure confidentiality in relation to patient data covered by the Access to Health Records Act 1990 and in all matters relating to the Data Protection Act 1998 and GDPR 2018.
- Any breach of copyright laws, for example in relation to protected commercial software, intellectual property or any other proprietary interest belonging to the University College.
- Deliberate unauthorised access to networked facilities or services.
- Attempting to circumvent or disable firewalls, security software or any security measures designed to protect systems against harm including monitoring and filtering.
- Use of privileged or administrative accounts to bypass monitoring, filtering or other security controls.
- Use of proxy avoidance, anonymous web browsers, VPNs and other methods for illegal streaming or similarly illicit activities.
- Attempting to make, run, use or store unlicensed copies of any software.
- Use of bit torrents for downloading and/or sharing illegal or copyright protected materials.
- Purposefully sending or forwarding any malicious content such as, but not limited to spam, phishing, malware, worms, Trojan horses, viruses and ransomware. Failing to take reasonable precautions to prevent the introduction of any such harmful program.
- The use of hacking tools which may lead to disciplinary action being taken.
- Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
  - Wasting staff effort or IT resources.
  - Corrupting or destroying other users' data.

    - Violating the privacy of other users.
    - Disrupting the work of other users.
    - Denying service to other users (for example, by overloading of access links or switching equipment, or of services or end systems).
    - Continuing to use an item of software or hardware after having been requested that use cease by IT or managerial staff because it is causing disruption to the correct functioning of IT systems.
    - Causing any loss – reputational, financial or of other resources.
  - Any other misuse, with intent to cause harm to the University College and/or its IT facilities and resources.

7.2 To avoid unintentional breach of this policy, the following must also be adhered to at all times:

- It is the user's responsibility to ensure that they log out of computers at the end of each session. It is also important to remember to log out of each individual resource (i.e. website) after use, otherwise sessions will remain open and are at risk of compromise.
- Users must lock their workstation when leaving their desk unattended.
- Users must not divulge their password or share their login credentials with other users under any circumstances. Passwords must not be written down in insecure locations.
- Users must not interfere with, damage or remove any IT equipment from the University College without permission from the Head of IT.
- Users must not disconnect or connect equipment from the network without permission from the Head of IT.
- Only IT staff may install or authorise the installation of software on any computer system. Any breach of this instruction is likely to breach licensing agreements and can be dealt with by FAST (Federation Against Software Theft).
- Users must ensure that protected, personal, sensitive or confidential data is not sent by any unencrypted or insecure means.
- Users should endeavour to be cyber aware, and must attend any mandatory Cyber Security training and pay attention to any updated guidance intended to promote awareness of new trends and threats.

8 Email

8.1 Most users will be provided with an AECC University College email address for exclusive use to fulfil their academic, administrative or research related duties. Email is a powerful tool with unregulated access posing additional threats to the institution as well as the user.

8.2 Email is the official communication medium for course and business matters.

8.3 Students must use email within the guidelines within the Student Handbook and Student Agreement. Interns in particular should ensure they utilise email to portray a professional image.

8.4 Staff must use email in accordance with AECC University College Brand Guidelines and Communications Policy – located on the S drive in the Marketing Public folder. In particular staff should configure their email signature as defined within these guidelines. Staff should set an appropriate out of office reply to cover absences of one day or longer.

8.5 Users must take great care to ensure the email addresses of recipients are entered correctly.

8.6 Email is not secure and must not be used for transmitting any personal identifiable or otherwise sensitive information. Guidance for secure transmission of personal or confidential information should be sought from the IT Team.

8.7 Users should treat all email attachments with care and must not open any attachments sent from an unfamiliar source. Any suspicious emails should not be opened and should be deleted immediately. If a suspicious file is unintentionally opened, change your password immediately and contact the IT Team.

9 Social Media

9.1 The use of social media, blogs and other similar sites is permitted for genuine AECC University College related purposes. Care must be taken and advice sought from the IT Team over security issues where these are evident or uncertain.

9.2 When using such websites, including personally in any connection with AECC University College, users must not perform any of the prohibited actions in section 7 of this policy. Specifically users must not disclose personal, confidential or sensitive information, write about the University College in a negative manner, or conduct themselves in a way that is detrimental to the University College or brings the University College into disrepute.

9.3 If employees are asked to contribute to an official blog or newsfeed connected to the University College, then special rules apply and advice must be sought from relevant senior staff and the Marketing Team.

9.4 Staff should consult with the Head of Marketing and Communications should they wish to establish new social media channels or platforms.

10 Exceptions

10.1 It may be permissible for activities which might be subject to legislation to be carried out in pursuit of legitimate, approved academic research (for example, work involving the use of images which may be considered indecent). In such cases users must ensure they have the written approval of their Head of Department and notify the Head of IT prior to commencement of such activities.

11 Monitoring Compliance

11.1 The University College IT Team will monitor the use of IT facilities in accordance with legislation and appropriate regulations. The purpose of this monitoring is to:

- Help ensure that IT facilities are available for the benefit of all authorised users without any undue interruption.
- Identify bottlenecks, overloads, weaknesses and hardware faults to be addressed before causing issues as well as contributing to system improvements.
- Identify insecure and vulnerable systems and block access to systems or services which may pose a threat or risk to network security and integrity.
- Ensure there is no breach of confidentiality.
- Prevent and detect and malicious interference.
- Prevent and detect crime.
- To establish the existence of facts and to ascertain compliance with these and other relevant regulations.

11.2 Information that is collected and monitored includes, but is not limited to: network session connection times, Internet use, network traffic (flow and volume), disk utilisation, email storage (volume). Information on telephone, printing and photocopying usage is also collected and monitored (i.e. itemised bills: basic call details). Please also see AECC University College privacy notices.

11.3 No member of staff is permitted, as a matter of routine, to monitor or investigate an individual's use of University College IT facilities. However in the event of suspected misuse, or where a legitimate request is made by the police or other authority, AECC University College reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. AECC University College may also disconnect

network services and prevent access to the IT facilities without notice while investigations proceed.

11.4 It may be necessary for AECC University College to access to a user's files and mailbox to maintain operations during an employee's absence. Such access will be authorised by the employee's line manager and will be restricted to the information required for the relevant business matter. It may however be unavoidable for personal files and messages which are not password protected or are poorly filed to be viewed in these circumstances.

Version:	2.1
Approved by:	SMG
Originator/Author	Head of IT
Owner	Head of IT
Reference source	HE Exemplars, incorporating key content of Janet Acceptable Use Policy.
Date approved	6th July 2021
Effective from	6th July 2021
Review date	July 2022
Target	All IT users (all Staff, students & visitors)
Policy location	SIP, VLE, public website
Equality Impact	No direct impact