Acceptable Use Policy

Classification – *Internal*

JULY 2025

ARDEN UNIVERSITY

Introduction

The Acceptable Use policy is a sub-policy of the Information Security Policy and forms part of Arden University's ISMS.

This policy sets out the rules, responsibilities and behaviours expected from all users of Arden University's information, systems and other associated assets.
The University must comply with a new condition of registration coming into force from August 1st 2025 regarding Sexual Misconduct and Harassment. As part of that, we have created a new single source of information where you can find:

- any updated policy
- the new mechanism to report an alleged incident of Sexual Misconduct and/or Harassment
- information on the support on offer to students, staff and visitors of the University
- new training to raise awareness of how we are responding and expected conduct on campus.

To find out more, visit our website which will be regularly updated and reviewed by the relevant University teams. Please note, the reporting form is specifically for Sexual Misconduct and Harassment. For details on how to report other types of concerns, please refer to the Safeguarding and Complaints Policies.

About this policy

This policy should be read in conjunction with, amongst others:

- Information Security Policy
- Incident Reporting Policy

Who is covered by the policy?

This policy applies to all Arden employees any third parties or contracted individuals conducting work at or for the University and all registered students who are authorized to have access to Arden University's systems.

Policy responsibilities

- The Head of Cyber Security in consultation with the Head of Student Success and the Legal Team shall be responsible for reviewing this Policy to ensure that it meets the legal requirements and reflects best practice.
- Managers are responsible for ensuring that all team members are aware of this policy.

- All permanent, contracted and temporary staff are required to read and abide by this policy.
- All students of Arden University are required to read and abide by this policy.

Compliance with this policy

You must ensure that you read, understand and follow this policy.

Definitions

Authorised User means your use of the Login that will be provided to you.

Information Systems means Arden University's computer systems, including hardware and devices, the network in Arden University premises, software and applications including iLearn, other linked systems such as: assessment submission portals (Turnitin), Unitu and Library systems and the information contained within such systems. This list is not exhaustive.

Login means your user identification code and password.

Message Systems means the Email system and any other applications and platforms which allow you to publish your thoughts, opinions, comments and images including but not limited to, iLearn, Zoom, Microsoft Teams and Chat channels.

Official Accounts means any official Arden University Social Media accounts.

Social Media means the applications and platforms which allow you to publish your thoughts, opinions, comments and images to a public audience including but not limited to, WhatsApp, Facebook, Instagram, LinkedIn, Snapchat, Twitter, all other similar sites, applications and platforms, and any other Internet postings, including blogs.

Website means www.arden.ac.uk.

Key Principles

Identity Management & Multi-Factor Authentication

- You will be provided with a Login as part of our security procedures. Your use of this Login will make you an Authorised User. You are responsible for all acts carried out while accessing the IT System through your Login. You must not share or disclose your Login to any other person.

- Passwords must be changed on first login to the system and at agreed intervals in accordance with the Arden Password Policy
- Multi-Factor Authentication (MFA) is now active (and mandatory) on all Arden accounts. You will have 14 days following first login to provide details for MFA. Further details are provided via IT communications.
- If you know or suspect that anyone other than you knows your user identification code or password, you must promptly notify us via the incident reporting links (staff – link here, students – link here). We have the right to disable any user identification code or password, whether chosen by you or allocated by us, at any time, if in our reasonable opinion you have failed to comply with any of the provisions of this clause.
- Log out of all Arden University devices at the end of working day.

Access Control & Use of IT Systems

- Only an Authorised User may access and use the IT Systems and only in connection with your studies, research or employment at Arden University.
- You must not modify or attempt to modify any of the IT Systems without the prior written consent of IT Services. For the avoidance of doubt, modifying shall include loading or attempting to load software on any Arden University hardware.
- Any errors, faults losses or damage must be reported immediately to help@arden.ac.uk.
- Each individual system should only be used in accordance with the specific instructions for that system. For help or support in using any of the systems, please contact help@arden.ac.uk or visit our Website.
- Please ensure that you log off when you have finished using the IT System or any part of it, or when you are away from your computer to prevent an unauthorised user from gaining access to our IT Systems.
- Unauthorised access to the IT Systems or any part of it is a breach of this Policy and will be handled in accordance with the relevant Disciplinary Policy.
- IT Systems may be updated from time to time, and the content may change at any time.
- Where reasonably practicable we will notify all users of any planned down time for repairs and updates to the IT Systems and will use reasonable endeavours to schedule such work at a time to cause the least disruption to the fewest people. We do, however, reserve the right to carry out any work on the IT Systems or part of them at any time.

- Access control is monitored and limited, however if you believe you have access to a system, service or information that you do not require for the course of your study or employment you must inform IT Services immediately. Failure to do so constitutes a breach of information security and will be dealt with in accordance with the relevant disciplinary policy or contractual agreement.

Viruses and Malware

- If you become aware of a virus or any other issues with the IT Systems, you must inform IT Services immediately and follow any instructions that they give you.
- **Students only** - It is your responsibility to ensure that your own personal devices used to access the IT Systems, including but not limited to computers, tablets and smart phones, are reasonably protected from bugs and viruses using appropriate firewall and anti-virus software (for example ensuring that any updates or fixes are put in place as soon as they are released by the manufacturer). Due to the range of devices available we cannot recommend specific firewall or anti-virus software to use.
- **Staff only** – for use of personal devices please follow the requirements of the Remote Working policy and the Bring Your Own Device policy.

Use of Removeable Devices

- The University does not allow the use / connection of removable devices (such as portable hard drives, USB sticks and mobile devices) into the Arden provided devices or network connections (other than via WiFi connections for mobile devices)
- OneDrive and SharePoint are provided for employees to be able to save and share documentation for use with Arden provided devices or equipment within Arden Study Centres.
- Arden devices within Study Centres must not be disconnected and replaced with personal devices.

Use of Mobile devices

- You must comply with the Remote Working Policy and the Mobile Devices Policy.
- You are responsible to keep all assigned mobile devices (mobile phone, laptop, tablet) safe and secure. Immediately report any loss or damage to your device to servicedesk@arden.ac.uk.

- You must safely handle all assigned devices when travelling or commuting, never leave device visible in a parked vehicle, devices must never be left unattended in public.

Use of AI tools

- All AI use must adhere to laws and regulations with emphasis on data protection, intellectual property, and ethical standards.
- Only approved AI tools and websites are to be utilised. A list of which is available on the Information Security intranet site.
- All AI use, research, and development, must be done ethically, avoiding biases, ensuring fairness, transparency, and accountability.
- The use of AI tools to support educational purposes must follow the University's mission and values.
- The use of AI for assessment must be detailed and justified within the related documents, outputs must be referenced and conform to related University's policy on academic integrity.
- The use of AI for published work must be comply with the guidelines and regulations on the use of AI provided by the funder, conference, or publisher.
- All data collected/used in AI tools must comply with the University's Data Protection and Privacy policy.
- You must avoid uploading the following types of data to an AI tool:
    - Passwords/usernames
    - Personally identifiable information or sensitive or confidential data
    - Data that has not been properly anonymised
    - Data related to the University's Intellectual Property
    - Data protected by Copyright
    - Data that could result to the University's reputational damage
    - Data collected (not publicly accessible) without consent for use
- You must verify the accuracy and appropriateness of AI-generated information prior to use.
- You must not use AI for any harmful, malicious, unethical, or illegal activities, with emphasis on unauthorised use of confidential data, copyrighted material or unprotected IP, hacking, discrimination, spreading misleading information, conducting harmful experiments.
- All AI tools developed within the University must comply with Intellectual Property rights and Licensing agreements.
- See AI policy for further information.

Content Standards

- Whenever you make use of a feature that allows you to upload content to our IT Systems, or to make contact with other users of our IT Systems:

    - You must comply with the content standards set out in clause 10.6; and
    - You warrant that any such contribution does comply with those standards, and you will be liable to us and indemnify us for any breach of that warranty. This means you will be responsible for any loss or damage we suffer as a result of your breach of warranty.

- Information uploaded to IT Systems shall be non-confidential. Any content you upload to all-user facing elements of our IT Systems will be considered non-confidential and non-proprietary, and we have the right to use, copy, distribute and disclose to third parties any such content for any purpose.
- Disclosure of information. We have the right to disclose your identity to any third party who is claiming that any content posted or uploaded by you to our IT Systems constitutes a violation of their intellectual property rights, or of their right to privacy.
- We are not liable for your acts or omissions. We will not be responsible, or liable to any third party, for the content or accuracy of any content posted by you or any other user of our IT Systems.
- We have the right to remove or edit any of your content on our IT Systems. We have the right to remove or edit any posting you make on our IT Systems if, in our opinion, your post does not comply with the content standards set out below.
- These content standards apply to any and all material which you contribute to our IT Systems (contributions), and to any interactive services associated with it. You must comply with the following standards which apply to each part of any contribution as well as to it as a whole. Contributions must not:

    - Contain any material which is defamatory of any person;
    - Contain any material which is obscene, offensive, hateful or inflammatory;
    - Promote sexually explicit material;
    - Promote violence;
    - Promote discrimination based on race, sex, religion, nationality, disability, sexual orientation or age;
    - Infringe any copyright, database right or trade mark of any other person;
    - Be likely to deceive any person;
    - Be made in breach of any legal duty owed to a third party, such as a contractual duty to a duty of confidence;
    - Promote any illegal activity;

  - Be threatening, abusive or invade another's privacy, or cause annoyance, inconvenience or needless anxiety;
  - Be likely to harass, upset, embarrass, alarm or annoy any other person;
  - Be used to impersonate any person, or to misrepresent your identity or affiliation with any person;
  - Give the impression that they emanate from us, if this is not the case;
  - Advocate, promote or assist any unlawful act such as (by way of example only) copyright infringement or computer misuse; or
  - Promote or encourage extremist or terrorist views, as defined in the Prevent Duty.

Use of email and other messaging systems

- The Message Systems are available for communication and matters directly concerned with your studies, research or employment at Arden University. You should use the Message Systems in accordance with the following principles:

  - Messages and copies should only be sent to those for whom they are particularly relevant. You should be careful not to copy emails automatically to all those originally copied into the original message;
  - Hasty and/or abusive email messages should not be sent as this may cause upset, concern and/or misunderstanding;
  - Please take steps to preserve the confidentiality of email messages. If you receive any email message that is not intended for you, you should return such message to the sender;
  - Your email address can receive emails from anyone connected to the Internet. Anyone found with offensive, pornographic or any material related to radicalisation or terrorism on their computer will be subject to investigation in accordance with the relevant Disciplinary Policy;
  - Arden University will not tolerate the use of the Message Systems for unofficial or inappropriate purposes, including, but not limited to, messages which could constitute bullying, harassment or other detriment; on-line gambling; and/or personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters). Abuse of this policy may lead to action in accordance with the Student and/or Staff Disciplinary Policy;
  - You should not knowingly attach to emails, any files which may contain a virus, malware or spyware.

- Arden University reserves the right to monitor and access any or all areas of any IT Systems (including email and chat boxes) from time to time for legitimate business reasons (including ensuring compliance with its Policies) and training purposes. You should not therefore assume that any information held on University computers and/or accessed through University computers is private and confidential to you.

- If you receive an email from an unknown source, or "junk" email you should report this email via the 'report message' button and then delete this from your system immediately without opening, replying to or forwarding it as it may contain a virus.
- Emails may contain file attachments or links to websites. These should not be opened / clicked on unless they are received from a trusted source, i.e. from known University staff or representatives. If in doubt, click on the 'report message' button in Outlook for verification.
- Unwanted emails should be deleted regularly to prevent our servers from filling up. Please note that deleted emails are stored on the system for some time and can be accessed as part of any investigation.
- The University monitors all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Use the incident reporting process immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.
- The University uses Arden provided email as an official form of communication with all users. Accounts should be checked regularly to ensure no such communications are missed.
- The University does not permit the forwarding of any Arden University email to any other email addresses (e.g. personal Hotmail / Gmail or other email addresses).
- The University reserves the right to add appropriate disclaimers or relevant promotional material to e-mails that are sent out, as and when is deemed necessary by the University Executive Group.
- The University does not promote or provide for the use of WhatsApp groups for staff or students. Should WhatsApp groups be used this is solely at the risk of the individual students. Staff must not use WhatsApp for any University business or for contacting / interacting with students.

Internet Access

- Anyone believed to have been visiting unauthorised sites relating to pornographic, radicalisation, terrorism material or other non-study related material will be subject to disciplinary action in accordance with the relevant disciplinary policy or terms of contract. Offences of this nature may be referred to the Police if deemed necessary.

- Arden University reserves the right to remove your Internet access privileges. Should this decision be taken, Arden University will advise you of the reasons for this action.
- Please note that the main servers maintain a record of Internet access by user and these will be monitored as necessary and results regularly forwarded to relevant University personnel and the Police, if appropriate.

Use of Social Media

- Social Media should never be used in a way that breaches any of Arden University's other Policies. If your actions would breach any University Policy in another forum, they will also breach them when carried out in an online forum or via Social Media.
- You are personally responsible for what you communicate in Social Media and any posts may be accessible for a long time. Please remember deleting a post does not mean that the post has not been seen or recorded in some format.
- You should make it clear that any posts are your own personal opinion or interpretation and do not reflect the views of Arden University. You must not hold yourself out as being an authorised representative of Arden University without prior approval in writing from the Vice Chancellor or the Pro- Vice Chancellor (Academic).
- If you have been granted access to any official Arden University Social Media accounts, in relation to a specific role or course, the content of such Official Accounts must reflect the views of Arden University.
- For the avoidance of doubt, you should not use Social Media for any of the following non-exhaustive, purposes:

    - Breach any other Arden University policy;
    - Defame or disparage or damage the reputation of Arden University or its affiliates, staff, students, customers, clients, business partners, suppliers, vendors or other stakeholders;
    - Harass or bully University staff or other students in any way;
    - Breach any laws or ethical standards;
    - Breach any intellectual property rights;
    - Breach any duty of confidentiality; or
    - Breach any of the terms of use of the Social Media platform.

- Please report any breaches of this policy to Director of Student Experience.
- Should you breach any of the above Policies you will be subject to Disciplinary Action.

Students under the age of 18

- The University may occasionally admit students who are under the age of 18 at the start of their course. Special considerations apply, in addition to those above:
    - The parent or guardian of any Arden University student under the age 18 is deemed to be responsible for the student's compliance with all Arden University policies and regulations;
    - To ensure that all students have equal access to the teaching and support offered by Arden University, students who are under 18 will be granted access to the same IT Systems as other students. Although our systems have measures in place to restrict access to harmful content, we cannot guarantee that they will not accidentally access websites that are pornographic or otherwise offensive or disturbing through our network;
    - In certain circumstances those under the age of 18 are not considered, in the eyes of the law, to be competent to enter into a legal contract. Accordingly, parents/guardians must ensure that their child/ward does not use IT Systems to attempt to do so.
    - Individuals under 18 cannot lawfully purchase alcohol, and must not do so by using Arden University's IT Systems.

Monitoring, breaches and review of this policy

- In accordance with the law, Arden University reserves the right to intercept and monitor the IT Systems, all forms of electronic communications on its systems, including (without limitation), email messages and Social Media. This may be to monitor criminal or unauthorised use, viruses, threats to the computer system, or to ensure the effectiveness of its operations and compliance with Arden University's Policies and Procedures. Monitoring may be of either the content and/or the extent of use and be on a random basis or when Arden University has cause for concern.
- Although Arden University respects your personal privacy, electronic communication tools are provided primarily for study and work purposes and Arden University's IT Systems and resources should not be provided for personal use.

- This policy will be reviewed on at least an annual basis by the Head of Cyber Security, Head of Student Success and the Legal Team to ensure that it continues to be fit for purpose.

Communication and Awareness

- This policy will be available to all employees within the SharePoint intranet.
- This policy will be available to all students via iTrent.

Policy Name:	Acceptable Use Policy
Policy Reference:	ISMSPOL003
Approval Authority:	Information Security Governance Board
Last Approved:	31/07/2025
Version:	2.0
Responsible SMT Lead:	Rob Palfreman
Responsible Department:	IT / Legal
Policy Contact:	Head of Cyber Security
Review Frequency:	Annually
Policy Classification:	Internal

Record of Amendments

Date	Version Number	Details of Change	Approval
21/03/2023	0.1	Re-draft for ISO27001:2022 ISMS	
18/09/2023	0.2	Updated to include comments & changes	
30/08/2023	1	Approved	Information Security Governance Board
31/07/2025	2	Update to include an AI section and Use of Mobile Devices, minor updates to key principles. Addition of required E6 compliance paragraph.	Information Security Governance Board