

Acceptable Use Policy

Contents

1.	Introduction	3
2.	Purpose of this policy	3
3.	Roles and responsibilities.....	3
4.	Scope	4
5.	Acceptable Behaviour	5
6.	Unacceptable Behaviour	6
7.	Safeguarding & KCSIE	8
8.	Monitoring	9
9.	Reporting & Investigation	9
10.	Acceptance.....	10
11.	Data Retention Statement.....	10
12.	Policy Review and Ownership.....	11
13.	Linking Table.....	11
14.	Amendments Log	12

1. Introduction

This Acceptable Use Policy outlines the standards and responsibilities expected of all users of Wiltshire College & University Centre's IT systems, digital services and information assets. Its purpose is to ensure that technology is used safely, legally and effectively, supporting a secure and productive environment for learning, teaching and professional work.

The policy applies to everyone who accesses College systems including staff, students, contractors and visitors, whether on-site or remotely. It covers all devices, software, systems and online services provided or supported by the College, including personal devices when used to access College resources.

2. Purpose of this policy

This policy exists to safeguard individuals, protect College systems and ensure that digital resources are used appropriately and effectively. All users share responsibility for maintaining a secure and respectful digital environment at Wiltshire College & University Centre.

This policy supports the College in:

- Protecting its IT infrastructure from misuse, disruption, unauthorised access or security threats.
- Ensuring that technology and digital services are used in a lawful, ethical and responsible manner.
- Promoting a safe, inclusive and productive learning and working environment for students, staff and authorised partners.
- Ensuring compliance with statutory and regulatory requirements, including data protection legislation, cybersecurity standards and safeguarding obligations.

All users share responsibility for maintaining the confidentiality, integrity and availability of the College's digital environment.

3. Roles and responsibilities

Users are expected to read, understand & sign this policy as a condition of their use of Wiltshire College & University Centre systems. This policy is in place to protect staff & the reputation of the College. Breach of this policy may be treated as a disciplinary matter.

All users of Wiltshire College & University Centre IT systems and digital services share responsibility for maintaining a safe, secure and effective digital environment.

Users (including staff, students, contractors and visitors) are responsible for:

- Reading, understanding and complying with this Acceptable Use Policy and any related College policies.
- Using IT systems, devices and digital services responsibly, lawfully and for authorised purposes only.
- Protecting login credentials, devices and information from unauthorised access.
- Promptly reporting suspected misuse, security incidents, data breaches or safeguarding concerns through the appropriate College channels.

Managers and Supervisors are responsible for:

- Ensuring that individuals they manage are aware of this policy and their responsibilities under it.
- Taking appropriate action where misuse or non-compliance is suspected, in line with college procedures.
- Supporting investigations into suspected misuse or security incidents.

IT Services are responsible for:

- Providing and maintaining secure, reliable IT systems and digital services.
- Implementing proportionate technical controls, monitoring and security measures to protect College systems and users.
- Supporting investigations into suspected misuse or security incidents.

Safeguarding Leads are responsible for:

- Advising on and responding to safeguarding-related concerns arising from the use of digital systems.
- Ensuring that technology use supports the College's statutory safeguarding duties, including Keeping Children Safe in Education (KCSIE).
- Supporting investigations into suspected misuse.

4. Scope

This Acceptable Use Policy applies to all individuals who access, use or manage the IT systems, digital services, network resources or information assets of Wiltshire College & University Centre. This policy applies irrespective of geographic location and covers both onsite and remote use. All users are responsible for ensuring that their actions comply with this policy and with any associated College regulations and legal requirements.

This policy applies to:

- **All employees** of Wiltshire College & University Centre, including temporary, casual and agency staff.
- **All students**, whether fulltime, part-time, apprentices, distance learners or on workbased programmes.
- **Contractors, consultants, partners and third-party service providers** who are granted access to college systems or data.
- **Visitors, volunteers and guests** who are provided with temporary access to college networks or facilities.

The scope includes all forms of access to College IT services, including but not limited to:

- **College-owned devices** such as desktops, laptops, mobile devices and teaching technologies.
- **Personally owned devices** when used to connect to college systems (e.g., email, Wi-Fi, cloud services).
- **All digital platforms, systems and applications** provided or supported by the College, including cloud-based and third-party services.
- **All data** stored, processed or transmitted using College systems.

5. Acceptable Behaviour

Users of Wiltshire College & University Centre's IT systems are expected to use digital services responsibly, respectfully and in a manner that supports the College's educational, operational and professional objectives. Acceptable behaviour includes, but is not limited to, the following:

Use of IT Systems

- Using College devices, networks and online services for legitimate work, study, teaching or research purposes.
- Accessing only those systems, information and resources for which permission has been granted.
- Ensuring all use complies with college policies, UK law and relevant regulatory requirements.

Digital Communication

- Using digital communication tools in a professional, respectful and appropriate manner consistent with the College's standards of conduct.
- Ensuring all digital communications support legitimate learning, teaching, research or work activity, or constitute reasonable personal use that does not interfere with duties or the performance of college systems.
- Respecting the privacy and personal data of others when communicating digitally, including not sharing information about individuals without their knowledge or consent.
- Ensuring all communications remain lawful and responsible, and do not incur unnecessary cost, risk or reputational harm to the College.

Use of Equipment and Facilities

- Taking appropriate care of college-owned hardware, software and digital resources.
- Using equipment and systems in a manner that avoids damage, disruption or interference with normal operations.
- Following provided instructions when using specialist systems, laboratories or cloud services.
- Where personal devices are used to access College systems, users are responsible for ensuring those devices meet a minimum standard of security.

Appropriate Use of Internet and Online Services

- Accessing online content and services in support of study, work or reasonable personal use that does not interfere with duties or the performance of college systems.
- Respecting copyright and intellectual property rights when accessing, creating or sharing digital materials.
- Ensuring personal use of IT services remains lawful, responsible and does not incur unnecessary cost or risk to the College.

Data Protection and Confidentiality

- Handling personal and College data in accordance with data protection legislation and internal guidance.
- Taking reasonable steps to secure devices, accounts and information from unauthorised access. This includes using strong, unique passwords for all College accounts, not reusing passwords across personal and College services, and complying with Multi-Factor Authentication (MFA) requirements where enforced. MFA is a mandatory security control and must not be disabled, circumvented or opted out.
- Reporting any suspected data breaches, security incidents or losses of equipment promptly.

Cyber-Safe

- Remaining alert to phishing attempts, malicious emails and suspicious online activity and reporting concerns immediately.
- Using only authorised systems, services and software and avoiding the introduction of unapproved applications or media.

Copyright

- Users must respect intellectual property rights and copyright when accessing, creating, using or sharing digital content using College systems.
- Complying with copyright law, software licensing terms and College agreements.

Use of Artificial Intelligence

- Using AI tools only in support of legitimate learning, teaching, assessment, research or administrative activity, in accordance with college guidance.
- Being transparent about the use of AI-generated content where required, particularly in assessed work, in line with the College's academic integrity expectations.
- Using only AI tools and platforms that have been approved or permitted for use within the College environment and seeking guidance from IT Services where unsure.
- Ensuring that College data, personal data or confidential information is not entered into external or consumer-facing AI tools unless those tools have been assessed and approved for that purpose by IT Services.
- Checking all AI-generated content for accuracy, bias, safeguarding risk and copyright issues before use or distribution, recognising that AI tools can produce inaccurate, misleading, biased or infringing content.
- Understanding that AI-generated content remains the responsibility of the individual who produces, uses or shares it. For staff, this includes reports, references, correspondence and other work-related communications. For students, this includes coursework, assessments and any other submitted work. The use of AI does not remove or reduce individual accountability for the accuracy, appropriateness or consequences of that content.
- Ensuring that any use of AI in assessment complies with the relevant awarding organisation's regulations and assessment requirements, in addition to the College's own academic integrity expectations. Specific guidance on the use of AI in assessment, including what constitutes academic malpractice, is set out in the College's Academic Malpractice, Maladministration and Plagiarism Procedures.

6. Unacceptable Behaviour

Users must not engage in any activity that could compromise the security, integrity or reputation of Wiltshire College & University Centre, its systems or its community. The following behaviours are prohibited. This list is not exhaustive; any action that breaches College policy, UK law or reasonable standards of conduct may be considered unacceptable.

Misuse of IT Systems

- Attempting to access systems, data or accounts without proper authorisation.
- Sharing login details, passwords, authentication codes or allowing others to use personal accounts.
- Circumventing or attempting to bypass security controls, filters, monitoring systems or access restrictions.
- Introducing unapproved hardware, software or storage media that may pose security risks.

Digital Communication

- Sending messages that are threatening, abusive, harassing, discriminatory, fraudulent, defamatory or deliberately misleading.
- Distributing spam, chain letters, phishing content, malware or unauthorised mass communications.
- Using College systems for personal commercial gain, political campaigning or activities unrelated to legitimate work or study without prior approval.
- Accessing, creating or sharing content that is unlawful, offensive or otherwise incompatible with a safe and inclusive educational environment.
- Any use that brings, or is likely to bring, the College into disrepute.

Use of Equipment and Facilities

- Damaging or attempting to alter College-owned equipment, cabling or network infrastructure.
- Tampering with hardware configurations, security settings or system software.
- Using personal devices to access College systems where those devices do not meet the minimum-security standards, including devices that are jailbroken, unpatched or otherwise compromised.

Inappropriate Use of Internet and Online Services

- Accessing, creating, downloading or sharing online content that is unlawful, offensive, discriminatory, harassing, defamatory, extremist or otherwise incompatible with a professional and educational setting.
- Using internet or online services in a way that interferes with duties, learning activities or the performance, security or availability of college systems.
- Engaging in excessive or inappropriate personal use that results in unnecessary cost, risk or reputational harm to the College.
- Downloading, sharing or using digital materials in breach of copyright, licensing conditions or intellectual property rights.
- Using online services to distribute spam, phishing content, malware or other harmful or unauthorised material.
- Using College internet access or online platforms for personal commercial gain, political campaigning or activities unrelated to legitimate work or study without prior approval.

Data Protection and Confidentiality

- Accessing, storing, transmitting or sharing personal or confidential information without a legitimate and authorised purpose.
- Failing to protect sensitive information, including leaving devices unlocked or transmitting data using insecure methods.
- Attempting to deidentify audit logs, delete evidence or conceal digital activity.

Cyber-Safe

- Any action that could intentionally or recklessly damage, impair or disrupt College IT systems, services or networks.
- Creating, uploading or distributing malware, ransomware or other malicious code.
- Conducting activities that place excessive load on IT resources or interfere with normal operations (e.g. large-scale unauthorised downloads).

Copyright

- Downloading or sharing copyrighted materials without permission or a valid licence.
- Using unlicensed software or circumventing licensing controls.

- Copying, distributing or modifying digital content in breach of copyright law or College agreements.

Use of Artificial Intelligence

- Using AI tools to generate, distribute or amplify content that is harmful, misleading, discriminatory, offensive or otherwise incompatible with a professional and educational environment.
- Using AI for harassment, impersonation, manipulation or the generation of deepfakes or other harmful synthetic media.
- Entering personal data, confidential College information or sensitive data into AI tools without confirming those tools are approved for such use by IT Services.
- Using AI tools to circumvent security controls, generate malicious code, conduct social engineering or support any other activity prohibited under this policy.
- Where a breach involves an AI-related safeguarding concern including deepfakes or AI-generated intimate images this must be reported using the College's safeguarding procedures (MyConcern) in addition to being treated as a breach of this policy. Such incidents should not be treated as a conduct or IT matter alone.

7. Safeguarding & KCSIE

Misuse of technology is not simply an IT or conduct issue, it may itself be an indicator of abuse, exploitation, grooming, coercive behaviour or sexual harassment. Staff and students should be alert to this possibility and report concerns promptly, even where the primary issue appears technical in nature.

Wiltshire College & University Centre is committed to providing a safe digital environment for all learners, including those under eighteen and vulnerable adults. Use of College IT systems must support the College's statutory safeguarding duties, as set out in Keeping Children Safe in Education (KCSIE) and the Prevent duty under the Counter-Terrorism and Security Act 2015.

In line with this guidance, the College:

- Maintains appropriate filtering and monitoring systems to reduce exposure to harmful or inappropriate content, including content that promotes extremism, radicalisation or terrorist ideology.
- Expects all users to behave safely and responsibly online, recognising that online actions can have safeguarding implications for themselves and others.
- Requires staff and students to report any online behaviour, content or concerns that may present a safeguarding or Prevent risk through the appropriate College channels.
- Works closely with the Designated Safeguarding Lead (DSL) to ensure technology use supports wider safeguarding processes.

Deepfakes and AI-generated images

Creating, requesting, possessing or sharing deepfakes, AI-generated intimate images or other manipulated media of another person without their consent is a serious safeguarding matter. Staff and students must understand that an image or video being "fake" or AI-generated does not reduce its potential to cause harm, such material can still constitute abuse and must be reported and acted upon in the same way as genuine content. Any concern of this nature must be reported immediately using the College's safeguarding procedures (MyConcern), in addition to any other reporting requirements under this policy.

Online behaviour outside college

Online behaviour that takes place outside college premises, hours or systems may still be treated as a safeguarding or disciplinary matter where it affects the safety or wellbeing of a member of the College community. This applies regardless of when or where the behaviour occurred, or which device or platform was used.

Users must not engage in any online behaviour that could place children or vulnerable learners at risk, including accessing harmful content, engaging in harassment or circumventing safety controls.

8. Monitoring

The College may monitor, log and review activity across its digital environment, including but not limited to:

- Network traffic and access logs.
- Email, messaging and collaboration tools.
- Internet usage and website access.
- Authentication events and account activity.
- Use of College devices, applications and storage systems.
- Security alerts and automated threat-detection systems.

Monitoring may be automated or conducted by authorised staff and is undertaken to:

- Detect and prevent security incidents, cyber threats or misuse.
- Support investigations into alleged misconduct or safeguarding concerns.
- Ensure compliance with college policies, contractual agreements and legal obligations.
- Maintain the performance and reliability of IT services.
- Filtering and monitoring arrangements are reviewed at least annually (KCSiE 2026 requirement)

The College does not routinely access the content of personal communications unless required for a legitimate, lawful or operational purpose and approved through the appropriate internal process.

Monitoring activities are conducted in line with:

- The College's data protection policies.
- UK GDPR and Data Protection Act requirements.
- Principles of necessity, proportionality and minimal intrusion.

Information gathered during monitoring will be handled securely and accessed only by authorised personnel.

9. Reporting & Investigation

Users must report any suspected misuse, security incident, data breach or safeguarding concern immediately through the appropriate College channels.

The College will investigate alleged breaches of this policy fairly, confidentially and in line with established procedures.

Enforcement and Consequences of Misuse

Failure to comply with this Acceptable Use Policy may result in:

- Temporary or permanent restriction of IT access.
- Disciplinary action under staff or student disciplinary procedures.
- Termination of contracts or withdrawal of access for external users.
- Notification to relevant external authorities where required (e.g., police, regulatory bodies).
- Civil or criminal legal action, where applicable.

Sanctions will be applied proportionately, considering the nature and severity of the breach.

Appeals

Users have the right to challenge or appeal enforcement decisions through the College's established staff or student procedures.

10. Acceptance

Access to and use of Wiltshire College & University Centre IT systems, networks and digital services is conditional upon compliance with this Acceptable Use Policy.

For staff and students, acceptance of this policy may be recorded electronically or as part of induction, enrolment or periodic compliance processes. Contractors, visitors and other external users are deemed to accept this policy through their use of college systems.

By agreeing to this policy, I understand that:

- I am responsible for all activities conducted under my account and sharing login credentials is prohibited.
- Access to the IT network is a privilege and users must not attempt to bypass network security measures.
- It is the user's responsibility, not the College's, to back up any local files.
- WCUC will actively monitor network traffic, internet usage, user accounts and has the right to report and investigate any suspicious behaviour or access to inappropriate material internally or to the appropriate authorities.
- I understand I must follow the rules and/or guidance to ensure no risk to my safety or to the safety and security of WCUC IT systems.
- I have a duty to report any breaches of this policy to the IT team as soon as possible.
- I will not use WCUC equipment for excessive personal use.
- Any violation or attempted violation of this policy may lead to temporary or permanent exclusion from the IT systems and services.
- I accept full responsibility for adhering to this policy and the relevant policies listed above as applicable.
- I have read and understood all the related policies that are relevant to me.

11. Data Retention Statement

Wiltshire College & University Centre is committed to ensuring the data it collects and holds is in line with the ICO's guidance and meets Data Protection law. Where appropriate a Data Protection Impact Assessment will be undertaken as and when policies are updated, to ensure risks to the individual and College are considered and managed.

12. Policy Review and Ownership

This document is owned and managed by IT Services. The policy will be reviewed and amended as required and at least every two years by the Head of IT Services or appropriate substitute, and subject to approval by the College's Senior Leadership Team.

13. Linking Table

Policy / Document	Purpose	Relationship to this AUP	Primary Owner
Safeguarding and Child Protection Policy	Sets out the College's statutory safeguarding duties, including online safety for children and vulnerable adults.	Supports safeguarding by defining acceptable digital behaviour, monitoring and reporting obligations in line with KCSIE.	Designated Safeguarding Lead
Keeping Children Safe in Education (KCSIE)	Statutory guidance for safeguarding and promoting the welfare of children in education.	Operationalises KCSIE requirements relating to filtering, monitoring, online behaviour and reporting concerns.	Department for Education
Data Protection Policy	Explains how personal data is processed, stored and protected in line with UK GDPR and the Data Protection Act.	Sets behavioural expectations for handling personal and College data when using IT systems.	Data Protection Officer
Information Security Policy	Defines technical and organisational measures to protect College information and systems.	Complements security controls by setting user responsibilities and prohibiting risky behaviours.	IT Services
Staff Code of Conduct	Outlines professional standards expected of staff in their work for the College.	Applies those standards to digital conduct, communications and system use.	Human Resources
Staff Disciplinary Policy	Sets out the formal process for addressing staff conduct issues, including misconduct and gross misconduct.	Provides the disciplinary route through which breaches of this AUP by staff may be managed, including cases where technology misuse also raises a safeguarding concern.	Human Resources

Policy / Document	Purpose	Relationship to this AUP	Primary Owner
Student Behaviour / Disciplinary Policy	Sets expectations for student conduct and the process for addressing misconduct.	Breaches of this AUP by students may be investigated and sanctioned under this policy.	Student Services
Academic Malpractice, Maladministration and Plagiarism Procedures	Sets out procedures for handling academic malpractice, including specific guidance on the use of AI in assessed work	Provides detailed assessment-specific rules that sit alongside the general AI expectations in this AUP	Quality

14. Amendments Log

Version	Date of Issue	Amendment summary	Author(s)
V1.0	09/06/26	Updated to align with current acceptable use expectations, safeguarding guidance and the use of emerging technologies e.g. artificial intelligence.	Phil Lewis
V1.1	09/07/26	Updated Sections 5 and linking table. Specific guidance on the use of AI in assessment, including what constitutes academic malpractice, set out in the College's Academic Malpractice, Maladministration and Plagiarism Procedures.	Phil Lewis, input from Matt Bowler, Quality.
V1.2	24/07/26	Updated Sections 5, 6 and 7 following Safeguarding team review against KCSiE 2026 guidance. Key additions: technology misuse reframed as a potential indicator of abuse or safeguarding concern, new provisions on deepfakes and AI-generated intimate images.	Phil Lewis, input from Andrea Blackmore, Safeguarding.
V1.3	28/07/26	Updated Linking Table to include a reference to the Staff Disciplinary Policy, clarifying the relationship between AUP breaches and disciplinary action.	Phil Lewis with input from Gail Larkin, HR Director.

