IT ACCEPTABLE USE POLICY

Policy category:	Technology and Data Protection
Approved by:	Policy Review Group 21/08/2026
Policy owner:	Group Director of Digital Transformation and IT
Related Policies:	Artificial Intelligence Governance Policy, Child Protection and Safeguarding Policy Low Level Concerns Policy
Applicable to:	Staff, students, governors, contractors, agency workers, consultants, volunteers and visitors
Effective from:	21/08/2026
Next review date:	30/08/2027

Section	Summary of changes (examples only)	Date updated
1.	Substantive rewrite and expansion of the previous policy, increasing the structure from 5 to 15 sections. The revised policy provides clearer governance, more detailed user responsibilities, and updated requirements for cyber security, AI, data protection, monitoring, incident reporting, device use and breaches of policy.	21/08/2026

Contents

IT Acceptable Use Policy

1. **Introduction**

1.1 This policy defines the acceptable use of all information technology systems, devices, applications, services, networks, cloud platforms and digital resources owned, managed, hosted or operated by UCS Group. The policy provides a framework for the safe, secure, lawful and responsible use of technology and information and supports the Group's educational, research and operational objectives. This policy should be interpreted broadly and should be regarded as applying to new and emerging technologies that may not be explicitly referenced within this document.

1.2 The Group provides a wide range of digital services including Microsoft 365, Teams, Outlook, SharePoint, OneDrive, wireless networking, mobile technologies, artificial intelligence services and cloud-hosted applications. These systems represent a significant organisational investment and are critical to the delivery of teaching, learning, student support and business operations.

1.3 Access to Group systems is provided to support legitimate educational and business activities. Access to these services remains the property of UCS Group and may be withdrawn where there is evidence of misuse, non-compliance, safeguarding concerns, information security risks or breaches of Group policies.

1.4 Users are personally responsible for ensuring that their use of technology complies with applicable legislation, regulatory obligations, contractual requirements and Group policies. The failure to comply with these requirements may result in disciplinary action, withdrawal of access rights, financial recovery of losses or referral to external agencies where appropriate.

1.5 This policy applies whether systems are accessed on campus, from home, whilst travelling, through Group-owned devices, personally owned devices, cloud services or future digital platforms adopted by UCS Group.

2. Policy statement

2.1 UCS Group is committed to maintaining a secure, reliable, inclusive and innovative digital environment that supports students, staff and stakeholders. The Group recognises that technology underpins almost every aspect of teaching, learning and business operations and therefore seeks to ensure that systems remain safe, available and resilient.

2.2 The Group takes cyber security, safeguarding, information governance and data protection seriously and expects every user to contribute towards maintaining an environment where information and technology resources are protected appropriately.

2.3 Technology resources are provided primarily to support educational, research and operational activities. Limited personal use may be permitted provided that such use

does not interfere with business operations, breach policy requirements, increase risk to the Group or generate excessive costs.

2.4 Users are expected to demonstrate professionalism, integrity and good judgement when using Group systems and services. Technology usage should always align with the values, objectives and reputation of UCS Group.

2.5 The Group will provide appropriate support, training, monitoring, security controls and guidance to assist users in meeting their responsibilities under this policy.

3. Scope

3.1 This policy applies to all individuals who access, use, support or administer Group technology services. This includes students, staff, governors, contractors, consultants, agency workers, volunteers, visitors and any third parties granted access to Group systems.

3.2 The policy applies regardless of where access occurs. Users remain subject to this policy when working remotely, studying from home, travelling, attending external events or accessing Group resources through cloud services.

3.3 The policy applies to all technology resources including Microsoft 365, Outlook, Teams, SharePoint, OneDrive, learning management systems, telephony platforms, network infrastructure, internet services, Artificial Intelligence platforms approved by UCS Group, and mobile devices and endpoint technologies.

3.4 The requirements of this policy apply equally to Group-owned equipment and authorised personally owned devices that connect to Group systems.

4. Governance and responsibilities

4.1 The Senior Leadership Team is accountable for implementation of this policy and for ensuring that appropriate resources, controls and guidance are in place.

4.2 The Group Director of Digital Transformation & IT is the policy owner and is responsible for the secure operation of Group technology services, technical controls, operational guidance and periodic review of this policy.

4.3 The Data Protection Officer, Designated Safeguarding Lead, Governance Professional, People and Culture team and other relevant specialists will provide advice and assurance within their respective areas of responsibility.

4.4 Managers and system owners are responsible for ensuring that access is appropriate to users' roles, that users receive relevant guidance or training, and that access is reviewed, amended or withdrawn when no longer required.

4.5 Compliance with this policy will be monitored and reported through the Group's agreed management and governance arrangements.

5. User Responsibilities

5.1 All users are expected to act responsibly, professionally and ethically when using technology resources. Users should consider the potential impact their actions may have on students, colleagues, systems, information and the wider reputation of UCS Group.

5.2 Users are accountable for protecting and appropriately using their assigned accounts and credentials. Activity associated with an account may be considered during an investigation alongside all other relevant evidence and circumstances.

5.3 Users must protect the confidentiality, integrity and availability of information assets. Information should only be accessed where there is a legitimate educational, operational or business need.

5.4 Users are expected to comply with all relevant policies including those relating to Information Security, Data Protection, Safeguarding, Artificial Intelligence, Cyber Security and Codes of Conduct.

5.5 Users must take reasonable precautions to prevent accidental disclosure, unauthorised access, misuse, damage or destruction of information and technology resources.

5.6 Users are expected to complete mandatory cyber security, safeguarding, information governance and compliance training where required. Refusal or failure to complete mandatory training may result in restrictions being applied to Group systems.

5.7 Users who become aware of behaviour that may place Group information, services or individuals at risk must report their concerns immediately through the appropriate reporting channels.

6. Passwords and Authentication

6.1 Secure authentication controls represent one of the most important measures available to protect information and systems from unauthorised access. Users must therefore maintain appropriate standards of password security and account management.

6.2 Passwords, authentication applications, security tokens and Multi-Factor Authentication methods are issued solely for the use of the authorised individual and must never be shared with another person.

6.3 Users should create strong passwords that are difficult to guess and resistant to common attack techniques.

6.4 Passwords must not be written down in insecure locations, stored in unapproved applications or disclosed through email, messaging systems or telephone conversations.

6.5 Multi-Factor Authentication forms an important part of UCS College Group's security strategy. Users must not approve unexpected authentication requests and must immediately report suspicious login activity.

6.6 Any indication of account compromise, credential theft or unauthorised access must be reported immediately to IT Services.

6.7 UCS College Group reserves the right to suspend accounts, reset passwords, revoke active sessions and undertake investigations where account compromise is suspected.

6.8 Users must not access, attempt to access or search for systems, records or information unless authorised and required for a legitimate purpose.

6.9 Users must not use another person's account or permit another person to use their account. Shared or generic accounts may only be used where expressly approved, controlled and auditable.

6.10 Privileged or administrator access must only be used for authorised administrative purposes and must not be used for routine activity where a standard account is sufficient.

6.11 Access rights will be granted according to role and business need and may be reviewed, amended or withdrawn where roles change, access is no longer required or risk is identified.

6.12 Users must not attempt to circumvent access controls, elevate privileges, discover vulnerabilities or test system security unless expressly authorised to do so.

7. Email, Teams and Digital Communications

7.1 UCS Group provides a range of communication technologies to support education, collaboration and business operations. These services must be used professionally, respectfully and appropriately at all times.

7.2 Communications undertaken using Group systems should reflect the values and standards expected within an educational institution. Users must not create, store, transmit or publish material that could reasonably be regarded as offensive, abusive, discriminatory, threatening, defamatory or inappropriate.

7.3 Staff must maintain professional boundaries when communicating with students and should use approved Group systems for educational and business communications.

7.4 Users must remain vigilant against cyber security threats including phishing attacks, business email compromise, social engineering and malicious attachments.

7.5 Requests involving financial transactions, passwords, bank account changes, payment instructions or sensitive information must always be independently verified before action is taken.

7.6 Email messages, Teams chats and digital communications may constitute official business records and may be subject to retention, monitoring, disclosure, legal review or regulatory investigation.

7.7 The Group reserves the right to implement malware scanning, email filtering, communication monitoring and other protective technologies to safeguard users and systems.

8. Internet, Social Media and Online Safety

8.1 Internet access is provided to support teaching, learning, research, collaboration and business activities. Users are expected to use online resources responsibly and, in a manner, consistent with the objectives of UCS Group.

8.2 Users must not knowingly access, download, create, store or distribute material that is illegal, offensive, obscene, threatening, discriminatory, extremist or otherwise inappropriate.

8.3 The Group operates filtering and monitoring controls designed to protect students, staff and systems from illegal, harmful and inappropriate content and cyber security threats, including risks associated with dynamic, personalised and AI-generated content. Users must not attempt to disable, override, alter or bypass these controls.

8.4 In support of safeguarding responsibilities and the Prevent Duty, users must not access, create, promote or distribute extremist, terrorist or radicalising content.

8.5 Users must exercise care when engaging with social media and online platforms and must not use them in a manner that breaches Group policy, compromises confidentiality, creates safeguarding or security risk, or could reasonably bring the Group into disrepute. Staff must also comply with the Staff Use of Social Media Policy, including when using personal accounts where their activity may have a material connection with, or impact upon, the Group.

8.6 Users must not engage in cyberbullying, online harassment, intimidation, impersonation or behaviour that could reasonably cause distress to others.

8.7 Any safeguarding concerns, harmful online content or concerning behaviours identified through technology use must be reported immediately to the Safeguarding Team.

8.8 The effectiveness of the Group's filtering and monitoring arrangements will be reviewed at least once every academic year. The review will be led by the Group Vice Principal of Student Experience and DSL responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and IT support. The review identified

gaps and resulting actions will be documented and reported through the appropriate safeguarding and governance arrangements.

9. Artificial Intelligence (AI) and Emerging Technologies

9.1 Use of Artificial Intelligence and other emerging technologies must comply with the Group's Artificial Intelligence Governance Policy, approved-service requirements and related guidance.

9.2 Users must only use approved AI services for authorised purposes and must not connect unauthorised AI tools, applications, browser extensions, plug-ins or integrations to Group systems or data.

9.3 Personal, confidential, safeguarding-related, commercially sensitive, security-sensitive or restricted information must not be entered into an unauthorised AI service.

9.4 Users remain responsible for reviewing and validating AI outputs and for reporting AI-related security, data protection, safeguarding or misuse concerns through the appropriate route.

10. Information Security and Data Protection

10.1 UCS Group is committed to protecting the confidentiality, integrity and availability of information assets. All users have a responsibility to protect information from unauthorised access, disclosure, alteration, destruction or loss.

10.2 Information should only be accessed where there is a legitimate educational, operational or business requirement. Users must not seek access to information that is not required for authorised purposes.

10.3 Users must comply with applicable data protection legislation, including the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together with the Group's information governance policies and current regulatory guidance.

10.4 Personal information must be processed lawfully, fairly and transparently and should only be retained for as long as required.

10.5 Information classified as confidential, commercially sensitive, safeguarding-related or restricted must be protected using approved controls and procedures.

10.6 Information should be stored within approved systems including Microsoft 365, OneDrive, SharePoint and other authorised platforms.

10.7 Users must not disclose personal information or confidential information without appropriate authority.

10.8 Any actual or suspected data breach must be reported immediately through the Group's incident reporting process.

10.9 Users must manage digital records in accordance with the Group's records-management and retention requirements. Users must not deliberately delete, alter, conceal or move records to avoid authorised access, retention, disclosure, audit, investigation, Freedom of Information, data protection or legal obligations.

11. Devices, Software and Storage

11.1 Group-owned devices represent a significant organisational investment and must be protected from loss, theft, misuse and damage.

12.2 Users are responsible for ensuring that devices remain physically secure whenever they are in their possession.

12.3 Only approved software may be installed on Group-managed devices. The installation of unlicensed, unsupported or unauthorised software is prohibited.

12.4 Users must not disable, bypass or interfere with security controls including device management systems, antivirus technologies, encryption solutions or monitoring tools.

12.5 Users must not introduce malware, ransomware, malicious code or software designed to compromise systems.

12.6 Information should be stored within approved systems that provide appropriate backup, recovery and security controls.

12.7 Portable storage devices must not be used unless authorised. Where use is approved, only Group-approved devices may be used, and information must be handled in accordance with Group security and records-management requirements.

12.8 The Group reserves the right to remotely manage, update, lock or erase Group-owned devices where necessary to maintain compliance, security and operational effectiveness.

12.9 Lost or stolen devices must be reported immediately to IT Services.

12.10 Personally owned devices may only be used to access Group services where authorised and configured in accordance with Group security requirements. The Group may restrict or withdraw access from devices that do not meet those requirements.

12.11 Users must take reasonable steps to prevent unauthorised viewing or access when working remotely or in public places, including securing unattended devices and protecting confidential conversations and screens.

11.12 Group information must not be downloaded, copied or synchronised to personal devices, personal email accounts, personal cloud storage or unauthorised applications unless expressly permitted.

11.13 International travel or access from overseas may be subject to additional security requirements or prior approval were identified by Group guidance.

11.14 Any exception to this policy must be authorised in advance by the appropriate system or policy owner, supported by a documented business or educational need and subject to proportionate controls and review.

11.15 Security controls and restrictions will be implemented with due regard to accessibility, equality and reasonable-adjustment requirements. Users requiring an adjustment must use the relevant support or approval route rather than bypassing security controls.

11.16 Wearable technology with camera, video, audio recording, live-streaming, biometric, augmented-reality or surveillance capabilities must not be worn, activated or used on College premises unless authorised in advance by a member of the Group Senior Leadership Team. This includes smart glasses, body-worn cameras, AI-enabled wearable assistants and any similar future devices. Authorisation will only be granted where there is a clear educational, operational, accessibility, health and safety or business need, supported by appropriate privacy, security and data protection safeguards. Any unauthorised recording, live-streaming or surveillance must be reported immediately to IT Services and, where relevant, the Safeguarding Team, Data Protection Officer or appropriate senior manager.

12. Incident Reporting and Response

12.1 Prompt reporting of incidents is essential to minimise disruption, support recovery activities and ensure compliance with legal and regulatory obligations.

12.2 The following incidents must be reported immediately: data breaches; lost or stolen devices; malware infections; account compromise; phishing attacks; safeguarding concerns; unauthorised access attempts; and technology misuse.

12.3 Where a user believes a device, account or system has been compromised, they should cease using the affected service where appropriate, preserve evidence and report the incident without delay.

12.4 Staff should report incidents through the IT Service Desk.

12.5 Students should report incidents to IT Services, their Tutor, Course Leader or the Safeguarding Team as appropriate.

12.6 Incident reports should include relevant information such as dates, times, devices involved, systems affected, actions already taken and any available evidence.

12.7 Upon receipt of a report, the Group may undertake containment, investigation, evidence preservation, recovery and remediation activities.

12.8 Suspected personal data breaches will be escalated immediately to the Data Protection Officer and relevant senior managers for assessment and reporting where required.

12.9 The Group may suspend access, isolate devices, reset passwords, block services or take other protective action where necessary.

12.10 The Group actively supports a culture of responsible reporting. Individuals who report concerns in good faith will not be disadvantaged.

12.11 The deliberate concealment of incidents or failure to report serious concerns may constitute a breach of this policy.

13. Monitoring, Filtering and Audit

13.1 The Group may operate proportionate monitoring, logging, filtering, auditing and security controls across its digital environment to support safeguarding, cyber security, legal and regulatory compliance, service management, incident investigation and business continuity.

13.2 Monitoring may be undertaken only for specified and legitimate purposes, on an appropriate lawful basis, and in accordance with relevant privacy information, retention requirements and access controls.

13.3 Users will be informed through the relevant Staff, Student and other applicable Privacy Notices, together with supporting policies and guidance, about the nature and purpose of monitoring, the categories of information that may be collected or reviewed, retention arrangements and how their rights may be exercised.

13.4 Monitoring may include authentication records, network and internet activity, email and communication metadata or content where authorised, device compliance information, security alerts, audit logs and incident evidence.

13.5 Monitoring arrangements will be necessary, proportionate and subject to periodic review. Information obtained through monitoring must not be used for an unrelated purpose without appropriate authority and consideration of the legal, employment, equality and ethical implications.

13.6 Information stored within Group systems remains the property of UCS Group and may be reviewed, searched or disclosed where there is a legitimate and authorised business reason.

13.7 Access to audit information and monitoring systems is restricted to authorised personnel acting within their professional responsibilities.

13.8 The Group may be required to disclose information to law enforcement agencies, regulators or other authorised bodies where legally required.

13.9 Management will provide periodic assurance on implementation of this policy through the Group's agreed governance arrangements. Reporting may include material incidents and trends, significant control weaknesses, policy exceptions, training completion, access reviews, filtering and monitoring assurance, audit findings and overdue corrective actions.

13.10 Material incidents or uncontrolled risks must be escalated promptly rather than awaiting routine reporting.

14. Breaches of Policy

14.1 The Group treats breaches of acceptable use, information security, safeguarding requirements and legal obligations seriously.

14.2 All alleged breaches will be investigated fairly, proportionately and consistently in accordance with applicable procedures.

14.3 The Group may take immediate action to protect systems, information and individuals where risks are identified. This may include suspension of accounts, restriction of access rights, device isolation or other security measures.

14.4 For students, breaches may result in action under the applicable Student Disciplinary Procedure, Student Code of Conduct, Academic Regulations or other relevant learner conduct procedures.

14.5 For staff, breaches may result in action under applicable employment policies, disciplinary procedures, information governance procedures, low level concerns policy or contractual arrangements.

14.6 Certain activities may constitute criminal offences and may be referred to law enforcement agencies for investigation.

14.7 Users who knowingly conceal incidents, destroy evidence, obstruct investigations or provide misleading information may be subject to disciplinary action.

14.8 The Group reserves the right to seek recovery of losses arising from deliberate misuse of technology resources where permitted by law.

15. Policy Review

15.1 This policy will be reviewed by the Group Director of Digital Transformation & IT at least annually or sooner where changes in legislation, cyber security risks, technology, operational requirements or regulatory obligations require amendment.

15.2 The policy will be approved through the Group's policy governance process and communicated to relevant stakeholders.

15.3 Users may be required to reconfirm acceptance of the policy following significant amendments as a condition of continued access to Group systems.

15.4 This policy should be read alongside the Group's current policies and procedures relating to Artificial Intelligence, data protection, information security, cyber security, safeguarding, online safety, records management, social media, mobile devices, equality, disciplinary matters, business continuity and whistleblowing.

User Acknowledgement

This policy forms part of the Group's governance framework and applies to all persons within its scope. The Group will communicate the policy through appropriate induction, training, guidance, contractual, academic and system-access arrangements. Where proportionate to the risk or type of access, users may be required to confirm that they have read and understood the policy.

Failure to comply with this policy may result in disciplinary action, withdrawal of access rights and, where appropriate, referral to external authorities.