ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE POLICY

Policy category:	Technology and Data Protection
Approved by and when:	Policy Review Group 21/08/2025
Policy owner:	Group Director of Digital Transformation and IT
Applicable to:	Staff, students, governors, contractors, agency workers, consultants, volunteers and visitors
Effective from:	21/08/2026
Review date:	30/08/2027

Document Version Control 1 – Revision History

Section	Summary of changes	Date updated
1	Major revision and expansion of the policy to establish a comprehensive AI governance framework. Includes updated governance arrangements, strengthened risk and compliance controls, clearer guidance on AI usage and alignment with emerging best practice, legal requirements and organisational objectives.	21/08/2026

Contents

Section	Section Heading	Page
1.	Introduction	3
2.	Policy statement	3
3.	Scope	3
4.	Definitions	4
5.	AI Governance Principles	4
6.	Approved AI Services and Authorised Use	5
7.	Governance, Roles and Accountability	6
8.	User Responsibilities	7
9.	Staff Use of AI	7
10.	Student Use of AI and Academic Integrity	8
11.	Data Protection, Confidentiality and Security	8
12.	Safeguarding, Online Safety and Inclusion	9
13.	Intellectual Property, Copyright and Records	9
14.	Procurement, Third-Party AI Services and Risk Assessment	10
15.	Human Oversight, Accuracy and Quality Assurance	11
16.	Prohibited and High-Risk Uses	11
17.	Incident Reporting and Response	12
18.	Monitoring, Audit and Assurance	12
19.	Training, Awareness and AI Literacy	13
20.	Breaches of Policy	14
21.	Policy Review	14
22.	User Acknowledgement	15

Artificial Intelligence (AI) Governance Policy

1. Introduction

1.1 This policy defines the safe, secure, lawful, ethical and responsible use of Artificial Intelligence technologies across UCS Group. It provides a governance framework for the use, development, procurement and oversight of AI systems used to support teaching, learning, student support, research, administration and business operations.

1.2 The Group recognises that AI technologies, including generative AI, machine learning, automation, decision-support tools and embedded AI features within cloud platforms, are becoming an increasingly important part of education and organisational productivity. Used appropriately, AI can support innovation, accessibility, efficiency, creativity and improved service delivery.

1.3 The use of AI also introduces risks relating to privacy, safeguarding, cyber security, bias, misinformation, academic integrity, intellectual property, transparency, over-reliance, reputational harm and compliance with legal or regulatory obligations. This policy therefore establishes clear expectations for all users and requires proportionate controls to be applied before AI is used in higher-risk contexts.

1.4 This policy should be interpreted broadly and should apply to AI technologies whether they are standalone products, embedded within approved business systems, accessed through public websites, integrated into teaching platforms, or provided through future digital services adopted by UCS Group.

2. Policy Statement

2.1 UCS Group is committed to enabling responsible innovation through AI while protecting students, staff, information assets, systems, safeguarding responsibilities and the reputation of the Group.

2.2 AI must be used in a way that supports the Group's educational objectives, complies with applicable legislation and policies, respects the rights and dignity of individuals, and maintains public trust in the Group's services.

2.3 Users are expected to demonstrate professionalism, integrity and good judgement when using AI. AI outputs must not be treated as automatically accurate, impartial, lawful, appropriate or fit for use without suitable human review.

2.4 The Group will provide appropriate guidance, training, monitoring, approval routes and technical controls to support safe AI adoption. The Group may restrict, suspend or prohibit AI services where risks to safeguarding, security, privacy, intellectual property, equality, academic integrity or compliance are identified.

3. Scope

3.1 This policy applies to all individuals who access, use, support, administer, procure, develop or make decisions using AI services on behalf of UCS Group. This includes students, staff, governors, contractors, consultants, agency workers, volunteers, visitors and third parties granted access to Group systems or data.

3.2 The policy applies whether AI is used on campus, remotely, during work or study, through Group-owned devices, personally owned devices, approved cloud platforms, public AI tools, mobile applications, browser extensions, plug-ins, integrations, APIs or third-party services.

3.3 The policy covers all AI technologies including but not limited to generative AI chatbots, image generation tools, text summarisation tools, transcription tools, code generation tools, automated marking or feedback tools, predictive analytics, decision-support tools, recommendation engines, AI-enabled search, AI agents and AI features embedded within Microsoft 365 or other approved platforms.

3.4 The requirements of this policy apply equally to experimental, pilot, trial, procured, internally developed and operational AI services.

4. Definitions

4.1 Artificial Intelligence means a technology or system that performs tasks normally requiring human judgement, reasoning, prediction, classification, language understanding, content generation, pattern recognition or decision support.

4.2 Generative AI means AI capable of producing new or transformed content, including text, images, audio, video, code, presentations, lesson materials, summaries, translations, plans, reports or other outputs in response to prompts or data.

4.3 Approved AI service means an AI service that has been authorised for use by UCS Group and is subject to appropriate security, data protection, procurement, contractual and governance controls.

4.4 Public AI service means an externally accessible AI service that is not formally approved by UCS Group and may process prompts, uploaded content, personal data, confidential information or usage data outside Group-controlled environments.

4.5 High-risk AI use means any AI use that could materially affect an individual's rights, access to services, assessment outcomes, safeguarding position, employment, progression, financial interests, wellbeing, privacy or legal status.

5. AI Governance Principles

5.1 Fairness: AI must not be used to create unfair conditions, discriminatory outcomes or unjustified barriers for students, staff or stakeholders.

5.2 Transparency: Users should be clear when AI has materially contributed to content, advice, analysis or decision support, particularly where the output is shared, published, assessed or relied upon by others.

5.3 Accountability: The person using AI remains responsible for the prompt, the data entered, the output used, the context in which it is applied and any resulting impact.

5.4 Privacy: AI must be used in a way that protects personal data, confidential information and the rights of individuals. Users must not enter personal, confidential, safeguarding or commercially sensitive information into unauthorised AI services.

5.5 Security: AI must not be used in a way that increases cyber security risk, exposes credentials, discloses system details, weakens controls or introduces malicious content.

5.6 Reliability: AI outputs must be reviewed, validated and cross-checked before use. Users must consider that AI can generate incorrect, misleading, incomplete, biased or fabricated content.

5.7 Inclusiveness: AI should be used to support accessibility, dignity, participation and inclusion. AI must not be used in a way that disadvantages individuals or groups.

5.8 Human oversight: AI must support human judgement rather than replace it in contexts involving welfare, safeguarding, assessment, employment, disciplinary action, access to services or other significant decisions.

5.9 Sustainability and proportionality: AI should be used where it provides a reasonable educational, operational, accessibility or public-value benefit. Adoption decisions should consider cost, duplication, resource use, environmental impact and whether a simpler non-AI solution would adequately meet the need.

6. AI Services and Authorised Use

6.1 Users may use AI technologies where permitted by Group guidance, academic regulations, contractual terms, professional standards and role-based authorisation.

6.2 AI services should be used through Group-managed accounts and approved configurations wherever possible so that appropriate security, data protection, retention and monitoring controls can be applied.

6.3 Users must not connect unauthorised AI tools, browser extensions, plug-ins, apps or integrations to Group systems, mailboxes, calendars, files, learning platforms or data sources without prior approval.

6.4 Use of public AI services for low-risk activities may be permitted where no personal, confidential, safeguarding, commercially sensitive, security-sensitive or restricted information is entered and where outputs are appropriately checked before use.

6.5 Where a user is unsure whether an AI service is approved, suitable or safe for a proposed use, they must seek guidance from IT Services, the Group Director of Digital

Transformation & IT, the Data Protection Officer or another relevant policy owner before proceeding.

6.6 The Group will maintain an Approved AI Services Register identifying services that are approved, restricted, under review or prohibited, together with any conditions applying to their use.

6.7 Material, novel or higher-risk uses of AI must be recorded in an AI Use-Case Register. The register will include the intended purpose, service, business owner, users, information involved, risk classification, assessments completed, approval decision, controls, review date and current status.

6.8 Staff must notify the policy owner where an approved service introduces a material AI feature, changes its processing arrangements or expands its permitted functionality.

6.9 Approval of an AI service does not constitute approval for every use. Users must comply with the permitted purposes, information classifications and conditions recorded for that service.

7. Governance, Roles and Accountability

7.1 The Corporation retains oversight of the Group's strategic approach to AI and its alignment with the Group's strategic objectives, values, risk appetite and legal and regulatory responsibilities.

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

7.3 The Group Director of Digital Transformation & IT is the policy owner and is responsible for maintaining the approved services and use-case registers, coordinating technical and supplier assurance, issuing operational guidance and overseeing proposed AI services and integrations.

7.4 The Data Protection Officer, Safeguarding Team, curriculum and quality leaders, Governance Professional and other relevant specialists will provide advice and assurance within their respective areas of responsibility.

7.5 The AI Committee will provide cross-functional oversight of AI adoption in accordance with its approved terms of reference, maintain oversight of the AI Use-Case Register and escalate matters outside its delegated authority. Given the strategic significance of Artificial Intelligence to UCS, any substantive change in AI adoption, governance, usage or user access must be approved by the Senior Management Team (SMT) prior to implementation.

8. User Responsibilities

8.1 All users are expected to act responsibly, professionally and ethically when using AI. Users should consider the potential impact of AI use on students, colleagues, systems, information, learning, assessment, safeguarding and the wider reputation of UCS Group.

8.2 Users are responsible for all AI activity undertaken using their accounts, devices, prompts, uploaded files, integrations or approved roles.

8.3 Users must protect the confidentiality, integrity and availability of information. Information should only be accessed, uploaded, processed or shared through AI where there is a legitimate educational, operational or business requirement and where the service is approved for that type of data.

8.4 Users must comply with relevant policies including those relating to acceptable use, data protection, information security, safeguarding, cyber security, academic integrity, records management, procurement, copyright and codes of conduct.

8.5 Users must take reasonable precautions to prevent accidental disclosure, unauthorised access, misuse, harm, damage or reputational risk arising from AI use.

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

9. Staff Use of AI

9.1 Staff may use approved AI tools to support productivity, planning, research, drafting, summarisation, accessibility, analysis, service improvement and teaching preparation where this is consistent with policy requirements and professional standards.

9.2 Staff must review, validate and, where appropriate, edit AI-generated content before using it in teaching materials, reports, communications, advice, business processes or operational decisions.

9.3 Staff must not use AI to make final decisions about students, applicants, staff, complaints, disciplinary matters, safeguarding cases, access to support, funding, progression, attendance interventions or other significant matters without appropriate human review and authorised governance.

9.4 Staff must maintain professional boundaries when using AI to communicate with or about students. AI must not be used to generate content that is misleading, inappropriate, discriminatory, intrusive or inconsistent with safeguarding responsibilities.

9.5 Staff using AI in teaching, learning or assessment contexts should provide clear guidance to students on permitted and prohibited use, including expectations for acknowledgement, originality, evidence and academic integrity.

10. Student Use of AI and Academic Integrity

10.1 Students may use AI where this is permitted by course requirements, assessment guidance, academic regulations and instructions provided by teaching staff.

10.2 Students remain responsible for ensuring that submitted work accurately reflects their own understanding, learning, effort and evidence. Presenting AI-generated content as wholly original work may constitute academic misconduct.

10.3 Students must not use AI to fabricate evidence, impersonate another person, falsify data, produce misleading references, bypass learning requirements or gain an unfair advantage.

10.4 Where AI has been used to support assessed work and disclosure is required, students must acknowledge the use of AI in line with the relevant assessment instructions.

10.5 Students must not enter personal information about themselves or others, safeguarding information, confidential College information, assessment materials not authorised for use, or details relating to other students or staff into unauthorised AI services.

11. Data Protection, Confidentiality and Security

11.1 AI use 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 all related Group information governance requirements and current regulatory guidance.

11.2 Personal data must be processed lawfully, fairly and transparently. Users must not enter personal data into AI services unless the service is approved for that purpose, there is a lawful basis, and appropriate controls are in place.

11.3 Confidential, commercially sensitive, safeguarding-related, security-sensitive or restricted information must only be processed through approved systems that provide appropriate contractual, technical and organisational safeguards.

11.4 Users must not upload documents, emails, student records, HR records, financial information, assessment information, credentials, system diagrams, security configurations or unpublished business information to unauthorised AI services.

11.5 AI prompts, outputs and uploaded files may constitute Group records. Where AI materially supports a formal decision, recommendation, assessment, investigation, published position or significant business activity, sufficient records must be retained in approved Group systems to explain the information used, the AI contribution, the human review undertaken, the decision reached and the person or body responsible.

11.6 Any actual or suspected disclosure of personal, confidential or restricted information through AI must be reported immediately through the Group's incident reporting process.

12. Safeguarding, Online Safety and inclusion

12.1 AI must be used in a manner consistent with the Group's safeguarding responsibilities, Prevent Duty obligations, online safety expectations and commitment to dignity, respect and inclusion.

12.2 Users must not use AI to create, access, promote or distribute harmful, abusive, threatening, discriminatory, extremist, radicalising, exploitative or otherwise inappropriate content.

12.3 AI must not be used to generate realistic images, audio, video, likenesses, impersonations or simulated communications of students, staff or other individuals without appropriate authority and a lawful, ethical and transparent purpose.

12.4 Any nude, semi-nude, intimate or sexualised image, video or other visual content involving or purporting to involve a child must be treated as a safeguarding concern, including where the content has been digitally altered or wholly generated using Artificial Intelligence and regardless of whether an authentic source image exists. Such content must be reported immediately and managed in accordance with the Group's safeguarding and child-on-child abuse procedures.

12.5 AI must not be used to profile, target, monitor or evaluate individuals in ways that could be intrusive, discriminatory, unsafe or inconsistent with safeguarding and equality duties.

12.6 Any AI-related activity, content or behavior that may present a safeguarding, welfare, online safety or wellbeing risk to a student, child or vulnerable adult must be treated as a safeguarding concern and reported immediately in accordance with the Group's Safeguarding Procedures. This includes harmful AI-generated content, impersonation, deepfakes, exploitation, grooming indicators, bullying, harassment, extremist content, self-harm related content, or any behavior that could place an individual at risk. Where relevant, IT Services must also be informed to support containment, investigation and preservation of evidence.

12.7 Before approving an AI service for direct learner use, the Group must obtain proportionate assurance that its intended purpose and target users are clear; it is appropriate for the relevant age groups and needs; filtering, moderation and reporting arrangements are suitable; privacy and data-use arrangements are transparent; accessibility and SEND needs have been considered; risks to cognitive, emotional and social development, mental health and manipulation have been assessed; and staff retain effective oversight and can intervene where necessary.

13. Intellectual Property, Copyright and Records

13.1 Users must respect intellectual property, copyright, licensing and contractual obligations when using AI services. Content must not be uploaded to AI tools where doing so would breach copyright, license terms, confidentiality or contractual restrictions.

13.2 Users must not assume that AI-generated content is free from copyright, plagiarism, licensing restrictions, factual errors or third-party rights. AI outputs must be checked before publication or reuse.

13.3 Where AI is used to create or materially assist in the creation of content through approved Group systems for work or study purposes, ownership, retention and permitted reuse will be managed in accordance with Group policies, employment terms, academic regulations and applicable law.

13.4 AI-generated or AI-assisted content used in formal publications, policies, reports, teaching materials, public communications or assessed work should be appropriately reviewed, attributed or disclosed where required.

14. Procurement, Third-Party AI Services and Risk Assessment

14.1 AI services must not be procured, subscribed to, integrated, piloted at scale or used with Group data without appropriate governance review.

14.2 Procurement and adoption of AI services must consider information security, data protection, safeguarding, accessibility, equality, contractual terms, hosting location, retention, auditability, service resilience, intellectual property, supplier assurance and exit arrangements.

14.3 An initial AI risk screening must be completed before a new AI service, material AI feature, integration, pilot or use case is approved. The screening will determine the further assessments and approvals required. A Data Protection Impact Assessment must be completed where processing is likely to result in a high risk to individuals' rights and freedoms. Security, safeguarding, equality, accessibility, academic quality, procurement and other assessments must be completed where relevant. No higher-risk use may proceed until required assessments are complete, identified controls are implemented, residual risk is accepted by an authorised decision-maker and the approval is recorded.

14.4 Third-party suppliers must provide sufficient assurance that AI services used by the Group are secure, lawful, transparent, appropriately governed and suitable for the intended educational or business purpose.

14.5 The Group reserves the right to reject, suspend or remove AI services that do not meet required standards or that create unacceptable risk.

14.6 Where a required assessment identifies a risk that cannot be reduced to within the Group's agreed risk appetite, the proposed use must not proceed unless it is formally escalated and approved by the person or body holding the relevant authority.

14.7 Procurement and adoption decisions should also consider total cost, duplication with existing services, environmental implications, availability of proportionate non-AI alternatives and the evidence supporting claimed benefits.

15. Human Oversight, Accuracy and Quality Assurance

15.1 AI outputs must be treated as draft, advisory or assistive unless an approved governance process states otherwise. Users must apply professional judgement before relying on AI outputs.

15.2 Users must check AI outputs for accuracy, completeness, bias, context, appropriateness, legality, safeguarding implications, accessibility and alignment with Group policy before use.

15.3 AI must not be the sole basis for significant decisions affecting students, staff or stakeholders. Human review, documented rationale and appropriate authority must be applied where decisions could have material consequences.

15.4 Where AI is used to summarise meetings, communications, policies, student information or business records, users must verify that the summary is accurate and does not omit material context.

15.5 Where AI is used to generate code, configuration guidance, data analysis or technical advice, outputs must be reviewed by competent staff before implementation in Group systems.

16. Prohibited and High-Risk Uses

16.1 Users must not use AI to deliberately deceive, falsify information, impersonate others, fabricate evidence, generate misleading content, bypass controls, conceal wrongdoing or misrepresent the source or originality of work.

16.2 Users must not use AI to generate deepfakes, non-consensual likenesses, harmful content, discriminatory material, defamatory content, malicious code, phishing content, social engineering messages or content intended to compromise systems or individuals.

16.3 Users must not enter passwords, authentication codes, personal data, safeguarding information, confidential records, payment information, bank details, unpublished security information, commercially sensitive information or restricted records into unauthorised AI services.

16.4 AI systems that could negatively affect fundamental rights, safeguarding, access to education, assessment outcomes, employment, data security or the wellbeing of individuals will be treated as high risk and must not be used unless formally approved with appropriate controls.

16.5 Any proposed AI use that appears novel, sensitive, high impact or unclear must be escalated for review before implementation.

16.6 AI agents or systems capable of taking actions, accessing connected data sources, communicating externally, changing records, initiating transactions or operating with continuing permissions must not be enabled without explicit approval, defined access

controls, testing, logging, human supervision, an emergency suspension mechanism and a named accountable owner.

16.7 AI must not independently authorise payments, enter contractual commitments, make safeguarding determinations, amend authoritative learner or staff records, issue formal decisions or communicate externally on behalf of the Group unless a specifically approved process provides effective human authorisation and oversight.

17. Incident Reporting and Response

17.1 Prompt reporting of AI-related incidents is essential to minimise harm, contain risk, support recovery and ensure compliance with legal and regulatory obligations.

17.2 The following AI-related incidents must be reported immediately: unauthorised disclosure of personal or confidential information; use of unapproved AI with restricted data; harmful or discriminatory AI output; suspected academic misconduct involving AI; safeguarding concerns; AI-generated impersonation or deepfake content; AI-generated intimate imagery involving or purporting to involve a child; malicious AI-generated code or phishing content; inaccurate AI output used in a significant decision; or unauthorised AI integration with Group systems.

17.3 Staff should report AI-related technology, security or data incidents through the IT Service Desk and escalate suspected personal data breaches to the Data Protection Officer without delay.

17.4 Students should report AI-related concerns to IT Services, their Tutor, Course Leader or the Safeguarding Team immediately as appropriate.

17.5 Incident reports should include relevant information such as dates, times, AI service used, accounts involved, prompts or outputs where available, data entered, systems affected, individuals impacted, actions already taken and any available evidence.

17.6 Upon receipt of a report, the Group may undertake containment, investigation, evidence preservation, risk assessment, communication, remedial action and reporting to external bodies where required.

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

18. Monitoring, Audit and Assurance

18.1 To protect users, systems and information assets, UCS Group may operate monitoring, auditing and security controls across approved AI services and the wider digital environment.

18.2 Monitoring of AI use will 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. Users will be informed through appropriate privacy notices and guidance of the nature and purpose of monitoring and how to exercise relevant rights.

18.3 Monitoring activities may include the review of authentication records, service usage, prompts and outputs where available, audit logs, device compliance information, security alerts, communication records and incident evidence.

18.4 Monitoring is undertaken to support safeguarding, cyber security, operational effectiveness, legal compliance, incident investigation, quality assurance, academic integrity and business continuity activities.

18.5 Monitoring activities will be conducted proportionately and in accordance with applicable legislation, regulatory requirements and Group policies.

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

18.7 Monitoring information must not be used for an unrelated purpose without appropriate authority and consideration of the legal, ethical, employment and equality implications. Monitoring arrangements and access permissions will be reviewed periodically to ensure they remain necessary, proportionate and effective.

18.8 Management will provide periodic assurance on implementation of this policy through the Group's agreed governance arrangements.

18.9 Assurance reporting will be proportionate to the scale and risk of AI use and may include approved and restricted services; material use cases and pilots; high and residual risks; assessment and audit activity; incidents, breaches and near misses; policy exceptions; supplier issues; training completion; control effectiveness; expected and realised benefits; and relevant regulatory or sector developments.

18.10 Material incidents, uncontrolled high risks or significant policy exceptions must be escalated promptly through the relevant executive and governance routes rather than awaiting routine reporting.

18.11 The effectiveness of filtering and monitoring arrangements relevant to AI access and use will be reviewed as part of the Group's wider filtering and monitoring review at least once every academic year. The review will be led by the senior leadership team member responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and IT support, and an appropriate record of the review and resulting actions will be retained.

19. Training, Awareness and AI Literacy

19.1 The Group will promote AI literacy so that users understand the opportunities, limitations and risks associated with AI use.

19.2 All staff and governors must complete the AI awareness or training applicable to their role within the timescale set by the Group. Students will receive appropriate AI literacy education through induction, curriculum, tutorial or other relevant activity.

19.3 Staff involved in designing, procuring, approving or administering AI services must ensure they understand the governance, security, data protection and safeguarding implications of those services.

19.4 Guidance may be updated as AI technologies, legislation, regulatory expectations and educational practice evolve. Users are expected to follow current guidance issued by the Group.

19.5 Additional role-specific training is mandatory for individuals who procure, configure, approve, administer or own AI services, or who use AI in assessment, safeguarding, recruitment, employment, learner support, complaints, investigations or significant decision-making.

19.6 Training completion, identified capability gaps and planned improvement action will be monitored through the Group's assurance arrangements.

20. Breaches of Policy

20.1 The Group treats breaches of AI governance, acceptable use, information security, safeguarding requirements, academic integrity and legal obligations seriously.

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

20.3 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, removal of AI services, device isolation, withdrawal of access to systems or other protective measures.

20.4 For students, breaches may result in action under Student Disciplinary Procedures, Codes of Conduct, Academic Regulations or other relevant procedures.

20.5 For staff, breaches may result in action under employment policies, disciplinary procedures, information governance procedures, contractual arrangements or professional standards.

20.6 Certain activities may constitute criminal offences and may be referred to law enforcement agencies, regulators or other authorised bodies where appropriate.

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

20.8 The Group reserves the right to seek recovery of losses arising from deliberate misuse of AI technologies where permitted by law.

21. Policy review

21.1 This policy will be reviewed by the Group Director of Digital Transformation & IT at least annually or sooner where changes in legislation, regulatory expectations, cyber security

risks, AI technologies, operational requirements or educational practice require amendment.

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

21.3 Users may be required to reconfirm acceptance of the policy following significant amendments as a condition of continued access to Group systems, approved AI services or digital resources.

21.4 This policy should be read alongside the Group's current policies and procedures relating to acceptable use, data protection, information security, cyber security, safeguarding, online safety, equality, accessibility, academic integrity, assessment, records management, intellectual property, procurement, risk management, complaints, disciplinary matters and whistleblowing.

22. User Acknowledgement

22.1 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.

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