TITLE		REF [as per register]	VERSION
Artificial Intelligence (AI) Usage Policy		DEP001	V3
APPROVAL BODY: [as per policy register]		**DATE** [of approval]	**REVIEW DATE**
Corporation Board		20 October 2026	15 October 2027
LEAD PERSON	Group Director of Digital Education and Artificial Intelligence		
EQIA DATE	29 September 2026	**DPIA DATE**	29 September 2026

ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY

1. Policy Statement

1.1. Activate Learning recognises the transformative potential of artificial intelligence (AI) and commits to harnessing it for educational excellence and business efficacy.

1.2. The AI policy aims to govern the use of AI to:

- Foster innovation in teaching and learning
- Incorporate AI in business practices to develop efficiencies
- Ensure ethical and responsive AI use of Bring Your Own (BYO) AI tools
- Oversee the development of AI tools to support staff and students

1.3. This policy aligns with Activate Learning's commitment to empowering learning. At the heart of this are the principles of our Learning Philosophy and values which ensures our staff and learners have access to cutting-edge technology and training, developing their digital knowledge, skills, and mindsets.

2. Purpose

2.1. The AI policy intends to set out Activate Learning's approach to the use of Artificial Intelligence (AI) including guidelines and rules for the use of AI tools. Activate Learning's aim is to maximise the benefits of AI while reducing risks and ethical concerns.

2.2. Integrate AI into teaching, learning, and assessment

2.3. Integrate AI into research and administrative processes

2.4. Promote data-driven decision-making

2.5. Safeguard privacy and fairness

2.6. The use of AI aligns with our group's vision to achieve far-reaching, progressive change and impact through learning. Providing talent for business and transforming lives through our Learning Philosophy by empowering every learner to reach their full potential.

3. Scope

3.1. This policy applies to all AI use within and on behalf of Activate Learning:

- All staff and students
- AI related activities across all departments
- Processes involving data collection, analysis and deployment of AI solutions

4. Responsibilities

4.1. As users of BYO AI tools and services, we are all responsible for:

- Protecting the information, we share online

- Following relevant policies and procedures
- Ensuring advice, guidance and training is applied in operation

4.2. **The Group Director of Digital Education and AI** is responsible for:

- Setting up an AI Committee and Steering Group to govern and steer adoption of AI tools across the organisation including new AI development (Appendix B: Draft AI Committee ToR)
    - Implement and train appropriate AI tools to support teaching, learning, and assessment.
    - Explore how AI can promote organisational efficiency.

4.3. Group Executive Team and Governors are responsible for:

- Setting the strategic direction, intent priorities and risk appetite of AI at Activate Learning
- Ensuring appropriate governance, resources and investment are in place to support safe, ethical and effective AI adoption
- Providing executive sponsorship and leadership for AI enabled transformation across the organisation
- Providing challenge and scrutiny regarding AI strategy, investment, governance and organisational impact

4.4. **Directors, managers and team leaders** are responsible for:

- Ensuring their teams follow this policy and relevant procedures and guidelines, and
- Ensuring their teams maintain data protection when using BYO AI tools

4.5. **Digital Education Services and AI Team** are responsible for:

- Ensuring tools developed maintain data protection and strictly adhere to our organisational policies and procedures
- Providing advice, guidance and training about the use and/or misuse of AI

4.6. Human Accountability

4.6.1. Artificial Intelligence systems may support decision-making and professional practice but must not replace human judgement.

4.6.2. Responsibility for decisions, actions, communications, assessments, recommendations and interventions remains with the member of staff using the AI system.

4.6.3. Users must exercise professional judgement when reviewing AI-generated outputs and remain accountable for any content or decisions influenced by AI.

5. Commitment Statement

5.1. Activate Learning commits to:

- Safe, ethical and legitimate use of AI
- Transparency in AI decision making
- Regular guidance and training for staff and students
- Continuous improvement of AI solution development

5.2. Responsible AI Principles

Activate learning will apply the following principles to all AI activity:

- Human Accountability and Oversight
- Safety and safeguarding
- Privacy and data protection
- Fairness and inclusion
- Transparency and explainability
- Reliability and accuracy
- Security and resilience
- Continuous improvement and innovation

5.3. AI Applications

A list of recommended AI tools, and applications which can be used, can be found HERE.
This list is amended regularly, and applications may be removed at any time. It is your responsibility to check in advance of using any AI in the workplace that your chosen application is suitable for use. Please contact the Digital Education Services and AI team with any concerns or comments you may have regarding the use of any of the listed AI applications.

Government Guidance on AI Tools

The institution does not recognise any generative AI platform as automatically approved by virtue of being referenced by government guidance. All AI solutions, including but not limited to Microsoft Copilot, ChatGPT, Google Gemini, and sector-specific educational AI applications, shall be subject to institutional risk assessment, information governance review, procurement controls, and approval processes before organisational use.

Selection of AI products should align with Department for Education guidance, UK GDPR requirements, cybersecurity standards, safeguarding obligations, and the organisation's AI Risk Classification Framework.

5.3.1. AI Application Approval Criteria

AI applications will be assessed against:

- Data protection requirements
- Information security requirements
- Safeguarding considerations
- Accessibility requirements
- Fairness and bias considerations
- Supplier transparency
- Legal and regulatory compliance
- Age appropriate use

New AI applications and tools can be suggested. There will be an approval process for the usage of

these apps which will include the evaluation of the tools in terms of security and data protection regulations.

5.4. Use which is permitted

5.4.1. You may use Generative AI for the following tasks provided that any information gathered or content generated is only generated, reviewed and used in accordance with the rules set out in this Policy. Examples include, but is not limited to the following:

- Drafting and editing documents
- Producing presentations, slides and charts, podcasts, videos
- Generating content for social media posts, website articles and think pieces
- Brainstorming ideas
- Research assistance
- Analysing non personal data to extract data insights.
- Automating or streamlining repetitive administrative tasks

5.4.2. Transparency

Users should be open and transparent about significant use of AI where appropriate.

Where AI has materially influenced educational content, communications, reports or decision-making processes, users should be able to explain:

- Why AI was used
- How AI was used
- What human review was undertaken
- Where final decision remained human-led

5.4.3. When you use AI-based features, you understand and agree that:

- The content may not always be accurate. You should not rely on the content produced as the sole source of truth or factual information, or as a substitute for support and professional advice.
- You must evaluate the content for appropriateness and accuracy for your use before sharing content.

5.5. Use which is not permitted

This section outlines the types of text that are prohibited from being inputted into the textbox of any BYO AI chatbot, including copyrighted material, personal information, hate speech, illegal activity, explicit content, misinformation, and malicious code.

5.5.1. **Copyrighted Material:** Text from copyrighted books, articles, songs, online documentation, code repositories or other media without permission.

5.5.2. **Personal Information:** Names, addresses, phone numbers, health-related data, national insurance numbers, or any other personally identifiable information.

5.5.3. H**ate Speech:** Content promoting hate, discrimination, or violence against individuals or groups based on certain characteristics.

5.5.4. **Illegal Activity:** Text that encourages or promotes illegal activities, such as drug use,

hacking, or other criminal behaviour.

5.5.5. **Explicit Content:** Graphic violence, pornography, or other adult content.

5.5.6. **Misinformation:** Deliberately false or misleading information, such as impersonation of another individual or organisation.

5.5.7. **Malicious Code:** Text that includes or suggests malware, viruses, or harmful software.

5.5.8. **Synthetic Harmful Content:** digital content (text, images, video, or audio) created or manipulated using artificial intelligence (AI) and other technologies, which can cause various types of harm, with significant implications for privacy, security, misinformation and safeguarding.

6. Considerations, Risks and Limitations

6.1. Generative AI tools process vast amounts of data to generate responses, but they have significant limitations. It's crucial for students and staff to understand the opportunities, limitations, and ethical issues related to using these tools. As generative AI capabilities evolve, users must be aware of the following aspects:

6.2. **Privacy and data considerations**: whether a generative AI tool is designed to learn directly from its users' inputs or not, there are risks to privacy and intellectual property associated with the information that students and staff may enter. If sensitive or personal information or even commercially confidential information is entered into the AI tool, it could be shared on a wider basis, overtly or indirectly as the AI tool learns. Users must be aware of the risk of data breaches or privacy violations and exercise caution with the data that they input into the AI tool.

6.3. **Potential for bias**: generative AI tools produce answers based on information generated by humans which may contain societal biases and stereotypes which, in turn, may be replicated in the generative AI tool's response. This can affect decision-making, recommendations, and user experiences. Biased AI can lead to unfair outcomes, reinforcing existing inequalities. Users must be aware of this and critically evaluate AI-generated content.

6.4. **Inaccuracy and misinterpretation of information**: data and information contained within generative AI tools is gathered from a wide range of sources, including those which may be poorly referenced or incorrect. Unclear commands or information may also be misinterpreted by generative AI tools and produce incorrect, irrelevant, or out-of-date information. This means that accountability for the accuracy of information generated by these tools when transferred to another context lies with the user.

6.5. **Ethics codes:** users of generative AI tools should be aware that while ethics codes exist, they may not be embedded within all generative AI tools. Some AI tools may not transparently communicate whether they adhere to specific ethics codes. Users might find it challenging to verify this information independently.

6.6. **Plagiarism:** generative AI tools re-present information developed by others and so there is the risk of plagiarised content and/or copyright infringement being submitted by a user as their own, and artwork used by image generators may have been included without the creator's consent or license.

6.7. **Equity and inclusion:** AI technologies have the potential to perpetuate or exacerbate existing biases. The costs and limitations associated with some tools also mean that access and therefore the benefits may not be available to everyone.

6.8. **Accurate content:** AI is being increasingly used to create content and images that appear legitimate but could be used in a negative way. AI is also being used to simulate contact and conversations. This is a safeguarding risk and has the potential to cause harm.

6.9. **Age Restrictions**: Creators impose age restrictions to ensure fairness and safety, for example:

- Microsoft CoPilot – Activate Learning IT account holders must be over 18 years old to use Microsoft CoPilot in a secure way
- Google Gemini - users must be aged 13 years old or older in the UK, but parental consent is required for users under 18 if treated as an "Additional Service" in Google Workspace for Education.
- ChatGPT - users must be over 13 years old, but if they are under 18, written consent from a parent or carer must be provided to Open AI (the creators of ChatGPT).

6.10. Automated Decision-Making

AI systems must not be used as the sole basis for decisions affecting:

- Learner admissions
- Assessment outcomes
- Student progression
- Disciplinary action
- Safeguarding decisions
- Staff recruitment
- Staff performance management
- Wellbeing interventions

Appropriately qualified staff must review and approve such decisions.

6.11. AI Risk Management and Organisational Assurance

Activate Learning adopts a risk-based approach to Artificial Intelligence governance, ensuring that the level of assurance, oversight and control is proportionate to the potential impact of the AI activity.

The organisation recognises that effective AI governance is not solely focused on technology risk but on the wider organisational impact of AI adoption, including educational, operational, legal, ethical, regulatory and reputational considerations. AI-related risks will therefore be managed through the AI Governance Framework, AI Change Management and Transformation Programme, Operational Change processes and organisational risk management arrangements.

The objectives of AI risk management are to:

- Support safe and responsible innovation.
- Protect learners, staff and stakeholders.

- Reduce organisational exposure to AI-related risk.
- Ensure compliance with legal and regulatory obligations.
- Support organisational AI maturity.
- Enable evidence-based decision making.
- Maximise the benefits of AI whilst maintaining appropriate safeguards.

Organisational AI Risk Categories

The following risk categories shall be considered when assessing AI use cases, systems and services.

- Information governance and data protection risk – risks associated with personal data exposure, data misuse, data retention and residency, GDPR compliance
- Information security and cyber risk – risks associated with vulnerable learners, harmful content, manipulation, deepfakes and psychological or emotional harm
- Education and academic risk – risks associated with assessment integrity, academic misconduct, learner dependency, inaccurate educational content and curriculum quality
- Operational risk – risks associated with process disruption, poor implementation, lack of support arrangements, business continuity impacts and resource dependencies.
  AI Initiatives resulting in operational change should be reviewed through the Operational Change Team as part of implementation planning and organisational readiness assessment.
- Ethical and equality risk – risk associated with bias, hallucination, discrimination, lack of transparency, lack of explainability and inequitable access.
- Reputational risk – risk associated with public confidence, trust, misuse of AI technologies, regulatory criticism, negative stakeholder impact.

AI Risk Classification

All AI use cases should be classified according to organisational impact.

Classification	Description
Low	Limited impact, low sensitivity and low organisational risk
Medium	Potential impact on learning, services or business processes
High	Potential impact on individual, learners, staff or organisational decision making
Critical	Significant impact on vulnerable groups, sensitive data, regulatory compliance or organisational compliance

Additional Controls for High and Critical Risk AI

AI systems classified as High or Critical Risk may require:

- AI Governance and Transformation Committee review.
- Data Protection Impact Assessment (DPIA).
- Equality Impact Assessment (EqIA).

- Information Security review.
- Safeguarding review.
- Operational Change assessment.
- Pilot and evaluation period.
- Benefits realisation review.

Approval requirements shall be proportionate to risk and organisational impact.

AI Risk Monitoring

AI-related risk will be monitored through:

- AI incident reporting.
- Governance reviews.
- Internal audit activity.
- Operational Change reporting.
- AI maturity assessments.
- Risk register reviews.
- Supplier assurance reviews.

AI risks and emerging trends will be reported to the AI Committee and escalated to the Group Executive Team where appropriate.

6.12. Vulnerable Learners

Particular care should be exercised when AI tools are used with learners who may be vulnerable due to:

- Age
- Special educational needs and disabilities
- Mental health needs
- Safeguarding concerns
- Digital literacy levels

Staff should ensure AI use supports and does not negatively impact learner wellbeing, inclusion or safety.

7. Misuse of AI

7.1. **Academic Dishonesty (Plagiarism)**

Activate Learning employs Turnitin and the expertise of its staff to monitor potential misuse of AI in student assessments.

7.2. Any violation of this policy may be treated as a disciplinary issue. For students, misuse of AI could lead to the rejection of their assessment, potentially affecting their program completion.

7.3. Activate Learning's Assessment and Verification Policy includes guidelines on the use and misuse of AI in assessment submissions. These guidelines help students and staff

understand AI and the rules set by the Joint Council for Qualifications (JCQ) and Awarding Organisations regarding AI tools in assessment submissions.

7.4. The use of AI in student work must be properly identified and referenced. Examples of AI misuse by students include:

- Copying or paraphrasing sections of AI-generated content, making the work no longer their own.
- Copying or paraphrasing entire responses of AI-generated content.
- Using AI to complete parts of the assessment resulting in work that does not reflect their own efforts.
- Failing to acknowledge the use of AI tools when they have been used as a source of information.
- Incomplete or poor acknowledgment of AI tools.
- Submitting work with intentionally incomplete or misleading references or bibliographies.

7.5. Work submitted for assessments must be the students' own. This means ensuring that the final product is in their own words, not copied or paraphrased from another source such as an AI tool, and that the content reflects their own independent work.

7.6. Students and apprentices are expected to demonstrate their own knowledge, skills, and understanding as required for the qualification in question, as outlined in the qualification specification.

7.7. Any use of AI that prevents students from independently demonstrating their own attainment is likely to be considered malpractice. (JCQ, jcq.org.uk/exams-office/malpractice/artificial-intelligence/, 2023)

7.8. **AI Incident Reporting**

Any incident involving the inappropriate, unsafe or unintended use of AI should be reported promptly through the appropriate organisational channels.

Examples include:

- Personal data exposure
- Significant misinformation
- Harmful AI-generated content
- Bias or discrimination
- Unauthorised AI use
- Deepfake or impersonation activity
- Safeguarding concerns

Incidents may be referred to the AI Committee, Designated Safeguarding Lead, Data Protection Officer or Information Security Team as appropriate.

Organisational channels can include Service Desk or by email to the following:

digital@activatelearning.ac.uk

Resilience@activatelearning.ac.uk

8. Synthetic Harmful Content

Activate Learning prohibits the harmful use of Generative AI. As identified in the Online Safety Policy, Activate Learning recognises the transformative potential of Generative AI. However, these tools can be misused to generate “synthetic harmful content”.

8.1. Synthetic Harmful Content refers to digital content (text, images, video, or audio) created or manipulated using artificial intelligence (AI) and other technologies, which can cause various types of harm, with significant implications on privacy, security, misinformation and safeguarding. This will include, but is not limited to:

- Misinformation and Disinformation:
- AI-generated false information.
- Manipulated content to mislead or deceive.

8.2. Explicit Content:

- Synthetic Child Sexual Abuse Material (CSAM).
- Non-Consensual Intimate Images (NCII).

8.3. Identity and Privacy Violations:

- Deepfakes (realistic but fake videos, images and audio).
- AI-generated impersonations for fraud or identity theft.

8.4. Individuals are responsible for any misuse of AI tools or for using applications that fall outside the list of recommended apps. This accountability extends to ensuring compliance with organisational guidelines and safeguarding against the misuse of AI tools.

8.5. As stated in the Online Safety Policy, the use of synthetic harmful content will be dealt with in accordance with Activate Learnings Student Positive Behaviour Management Policy and Staff Professional Conduct Policy and may be reported to external agencies such as Social Care and Police if it is considered a criminal offence criminal offence or indicate a risk of harm to children or adults at risk.

8.6. Safeguarding

8.6.1. Synthetic harmful content should be treated as a safeguarding concern where it causes, or may cause, harm to a child, young person or vulnerable adult.

8.6.2. Any such concerns must be managed in accordance with the Safeguarding and Prevent Policy and Online Safety Policy.

9. Emerging Technologies

9.1. Activate Learning recognises that emerging technologies continue to evolve and create new opportunities for learning, communication, accessibility and operational efficiency. However, they may also introduce new safeguarding, privacy, security, ethical and legal risks.

9.2. For the purposes of this policy, emerging technologies include, but are not limited to:

- Artificial Intelligence (AI) systems
- Wearable technologies

- Smart glasses
- Smart watches
- Body-mounted cameras
- Extended Reality (XR), Virtual Reality (VR) and Augmented Reality (AR) technologies
- Internet of Things (IoT)
- Future technologies with recording, monitoring, communication or content generation capabilities.

9.3. Users must not use wearable or emerging technologies to record, livestream, photograph or otherwise capture images, audio or video of staff, visitors or contractors without appropriate authorisation and a lawful basis for doing so.

9.4. The covert recording of individuals, including through smart glasses, wearable devices or other existing or emerging technologies, is prohibited unless specifically authorised as part of an approved safeguarding, regulatory or investigative process.

Unauthorised covert recording may constitute:

- A safeguarding concern
- A disciplinary matter
- A breach of privacy or data protection legislation
- A criminal offence

9.5. The misuse of emerging technologies to harass, intimidate, exploit, impersonate, deceive, manipulate or facilitate abuse of another person is prohibited.

This includes the creation, modification, sharing or distribution of:

- AI-generated impersonations
- Deepfakes
- Synthetic media
- Deceptive audio, image or video content
- Non-consensual intimate imagery
- Any content intended to cause harm, distress or reputational damage

– Any safeguarding concerns arising from the use of emerging technologies must be reported immediately in accordance with the Safeguarding and Prevent and Online Safety Policy.

9.6. Activate Learning reserves the right to restrict, monitor, block or prohibit the use of emerging technologies where there is a risk to safeguarding, privacy, security, assessment integrity or organisational reputation.

9.7. The organisation will continue to review emerging technologies and update technical controls, guidance and training to ensure new developments are implemented safely, ethically and in accordance with legal, regulatory and organisation requirements.

10. Implementation, Oversight and Monitoring

AI Maturity and Continuous Improvement

Activate Learning will utilise recognised sector frameworks, including the Jisc AI Maturity Toolkit and the AoC Digital Transformation and AI Roadmap, to assess organisational progress, identify areas for improvement and support strategic decision-making. AI maturity assessments will inform governance priorities, capability development, risk reduction activities and future investment decisions.

10.1. Activate Learning reserves the right to monitor use of AI applications on its systems and to monitor other activities for potential misuse of AI by students or staff.

10.2. Any questions or issues arising from using AI should be referred to the AI Committee.

10.3. The AI Committee will advise the Group Executive Team (GET), Group Leadership Team (GLT) and Education Leadership Team (ELT) on the use of AI applications, ensuring alignment with technical developments and ethical guidelines and principles.

10.4. Any complaints or challenges about Activate Learning's use of AI or anything pertaining to this Policy should be addressed through the Complaints Policy and Procedure.

10.5. Audits of the use of AI systems will be conducted to assess their impact, identify potential issues, and ensure compliance with ethical standards.

10.6. AI Literacy

Staff using AI systems are expected to maintain appropriate levels of AI literacy and participate in training relevant to their role.

Training should include:

- Safe and ethical AI use
- Data protection
- Safeguarding
- Bias awareness
- Verification of AI outputs
- Responsible use of emerging technologies

References

This policy should be read in conjunction with the policies and guidance identified below, all policies can be found on SharePoint:

- Information Security and Data Protection Policy
- Acceptable Use Policy
- Assessment and Verification Policy
- Safeguarding and Prevent Policy
- Online Safety Policy
- Refer to the UK National AI Strategy[1] and ICO's AI and Data Protection Guidance[2].

Research undertaken to inform revisions:

Keeping Children Safe In Education 2026

Resources: digital transformation and AI… | Association of Colleges

AI maturity toolkit for tertiary education - Jisc

AI Risk Management Toolkit: guidance - GOV.UK

Essential digital skills standards: 2026 - GOV.UK

Appendix A – Responsible AI Use Framework

Principle	What This Means	Examples
1. Human Accountability and Oversight	AI can support decisions but must not replace professional judgement. Humans remain responsible for outcomes and decisions.	• A tutor uses AI to draft assignment feedback but checks and adapts it before issuing it. • AI identifies attendance concerns, but a member of staff decides whether intervention is required. • Managers review AI-generated reports before making decisions.
2. Safety and Safeguarding	AI use must support learner safety, wellbeing and protection from harm. Any safeguarding concerns linked to AI must be reported.	• Reporting deepfakes or AI-generated impersonation. • Escalating concerns about harmful chatbot conversations. • Reviewing AI-generated content before sharing with learners. • Considering risks to vulnerable learners before introducing AI tools.
3. Fairness, Equality and Inclusion	AI outputs should be reviewed for bias and discrimination. AI should promote inclusive learning and equitable access.	• Checking examples generated by AI for stereotypes. • Ensuring learning materials represent diverse perspectives. • Using AI tools that support translation, captions or accessibility features. • Reviewing automated recommendations for bias.
4. Privacy and Data Protection	Personal, confidential and sensitive information must be protected at all times.	• Never entering safeguarding records into public AI systems. • Removing identifiable learner data before analysis. • Only using approved AI platforms that meet organisational requirements. • Following GDPR and organisational policies.
5. Transparency and Explainability	Users should be able to explain how and why AI was used and what human review was applied.	• Declaring AI use in reports, learning resources or assessment materials

		where appropriate. • Explaining how AI contributed to a recommendation. • Retaining oversight of all final outputs.
6. Security and Information Governance	AI systems must be secure, approved and compliant with organisational requirements.	• Using approved AI systems only. • Following supplier approval processes. • Reporting suspicious AI behaviour or security concerns. • Applying strong password and account security practices.
7. Accuracy, Reliability and Verification	AI outputs must be checked for accuracy, relevance and appropriateness before use.	• Fact-checking AI-generated content. • Verifying references and citations. • Reviewing AI-generated lesson plans. • Cross-checking information against trusted sources.
8. Ethical Use and Professional Conduct	AI must not be used to deceive, manipulate, harass or cause harm. Organisational values apply to all AI use.	• Not creating deepfakes of colleagues or learners. • Not using AI to generate discriminatory content. • Using AI in ways that support learning rather than circumvent assessment rules. • Respecting copyright and intellectual property.
9. Innovation, Learning and AI Literacy	Staff and students should explore AI responsibly and continue developing their knowledge and skills.	• Participating in AI training. • Sharing effective practice with colleagues. • Testing new approaches through approved pilots. • Reflecting on benefits and risks of AI tools.
10. Continuous Monitoring, Improvement and Governance	AI use should be reviewed regularly to ensure safety, compliance, effectiveness and alignment with organisational values.	• Reviewing approved AI tool lists. • Conducting AI audits. • Monitoring incidents and trends. • Updating guidance and training in response to emerging risks.