Artificial Intelligence (AI) Governance Policy

Approved by RIAM Governance & Nominations Committee: 23rd June 2025
Approved by RIAM Governing Body: 10th July 2025

1. Context

1.1 The integration of artificial intelligence (AI) technologies has the potential to revolutionise teaching and learning, streamline administrative processes, and enhance overall operational efficiency.

1.2 Traditional AI systems are programmed with specific rules and algorithms. Generative AI refers to deep learning AI models which can take raw data and generate outputs in the form of text, images or video in response to specific prompts. Chat GPT, Midjourney, Google Bard and Runway are examples of Generative AI applications in common use.

1.3 The Royal Irish Academy of Music, hereinafter referred to as RIAM or the Academy, recognises the importance of adopting AI technologies to harness the potential benefits for the organisation while mitigating, in so far as practicable, the potential risks.

1.4 RIAM classifies AI systems according to the risk categories established by the EU AI Act, which distinguishes between unacceptable, high-risk, limited-risk, and minimal-risk AI systems. High-risk AI systems (e.g. those used for assessments, administrative decisions, or biometric identification) will require additional risk assessment before approval. Further guidance on these classifications are detailed in Section 6.2.3.

1.5 Staff and students, using AI-generated content must disclose its use when relevant (e.g. research, assignments, decision-making).

2. Purpose

2.1 The purpose of this policy is to provide RIAM with a framework to ensure the appropriate deployment, management and oversight of AI systems across the Academy.

2.2 This policy should be read in conjunction with existing relevant policies. This policy ensures that the use of AI aligns with ethical values, data protection laws, and RIAM policies. It should be read in conjunction with the relevant legislation and regulations mentioned in section 10, and the RIAM policies referenced in section 11.

2.3 The Academy reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy. Disciplinary actions could range from a written warning to termination of access rights to your RIAM account depending on the severity of the violation.

3. Scope

3.1 This policy applies to all personnel under the remit of the RIAM. Third parties supplying services which involve the use of AI-powered tools must comply with GDPR, the EU AI Act and this policy.

3.2 This policy applies to all uses of generative AI for business purposes. This means any work which is carried out during a staff member's duties, whether this be on a company-issued device or a personal device. This also means any assignments or projects submitted by students for assessment.

4. Benefits

4.1 This policy is intended to promote responsibility and equity in how AI tools are accessed, how AI-enabled learning experiences are designed, and how students apply AI in their studies.

4.2 The Academy encourages human-centric AI, ensuring AI systems are used to enhance learning and efficiency rather than replace human judgment. RIAM will periodically, and whenever necessary, assess AI's impact on student learning outcomes, administrative efficiency, and faculty support.

5. Principles

5.1 RIAM undertakes to perform its responsibilities under the relevant legislation.

5.2 RIAM reserves the right to limit authorised use of AI to a specific list of applications.

5.3 RIAM does not permit the inputting of any personal data, or any content which may be regarded as confidential, or any sensitive company information into an AI application.

5.4 AI systems should not be used for any activity autonomously for critical decision-making (e.g. admissions, grading, disciplinary actions). A human must always verify AI-generated results.

6. Policy

6.1 This Policy sets out the RIAM's policy and procedures which shall be followed when incorporating AI tools into teaching and learning.

6.2 The assessment of the suitability of particular AI applications will be based on the following assessment criteria:

6.2.1 Purpose and Value

The Academy will assess AI applications on the basis of their potential to offer suitable value to its work. Any proposed applications for authorised use will be evaluated on this basis in consultation with relevant stakeholders within the organisation.

6.2.2 Risk Management

The Academy will undertake a comprehensive risk analysis of any proposed AI application, with consideration given to risk relating to factors such as data security, potential biases, intellectual property rights and accuracy. Any risk assessment will be carried out in the context of the wider legal framework on Artificial Intelligence, namely the European Union Artificial Intelligence Act and the Assessment List for Trustworthy Artificial Intelligence (ALTAI).

6.2.3 EU AI Act

The Academy will assess AI systems based on their purpose, value, security, and compliance. RIAM will categorize AI systems into the following categories established by the EU AI Act:

- Minimal risk: Allowed without restrictions for all employees/ students
- Limited- risk: May be used but requires transparency that they are in use
- High-risk: Requires formal approval and human oversight before they can be used
- Prohibited: Any tool deemed unacceptable to use under the EU AI Act

6.2.4 Continuous Monitoring

The Academy will periodically and whenever necessary, perform AI Audits to ensure compliance and mitigate emerging risks associated with the onboarding of new AI tools. Any AI system onboarded by the Academy will be continuously monitored for any performance and security risks that may be present.

6.3 The authorisation of AI applications for business use is an iterative process, the authorisation of a particular application does not guarantee that it will remain approved indefinitely. Therefore, the Academy reserves the right to revoke authorisation for use of any authorised AI application.

6.4 The following AI applications are not permitted for use within the organisation ie AI systems:

- **deploying subliminal, manipulative, or deceptive techniques** to distort behaviour and impair informed decision-making, causing significant harm.
- **exploiting vulnerabilities** related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.
- **social scoring**, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.
- **assessing the risk of an individual committing criminal offenses** solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.
- **compiling facial recognition databases** by untargeted scraping of facial images from the internet or CCTV footage.
- **inferring emotions in workplaces or educational institutions**, except for medical or safety reasons.
- **biometric categorisation systems** inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.
- **'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement**

Any AI application included in this list will be blocked from use on the RIAM network via web filtering and firewall capabilities

6.5 Any requests to use an AI service on the blocked list must be approved in advance by the AI Approval Team. The approval of any special use case will only be given in exceptional circumstances and will not indicate an indefinite approval for said use.

6.6 Installation of all approved AI applications is controlled by the ICT Department so that there will be visibility of what AI-powered tools are being used in the Academy and thus avoid any potential risks to RIAM's reputation. This entails reviewing the tool's security features, data ownership, data localisation, privacy features, terms of service, and AI tool's publishers' policies are in line with RIAM's privacy and information security standard requirements.

6.7 The use of AI comes with inherent risks, including potential bias, inaccuracies, and ethical concerns. All users should use critical-thinking to evaluate AI-generated outputs before relying on them.

6.8 AI is an emerging technology and RIAM will endeavour to assist staff and students to incorporate these tools in their work through education and training.

7. Procedures

7.1 It is the duty of each staff member and student to comply with general guidelines on the use of Artificial Intelligence.

7.1.1 Confidentiality and Data Protection

Staff and students should refrain from inputting into an AI application any content which may be regarded as confidential or sensitive company information. Personal data (i.e. any data through which an individual may be identifiable) should not be inputted into AI. Personal data may refer to the data of other members of staff, students or third-party individuals such as clients and vendors. If there is confusion on what constitutes as personal information, RIAM urges personnel to contact the ICT Department for clarification on whether a specific piece of data is allowed to be processed by an AI system.

The following is a non-exhaustive list of data which should not be inputted into any AI application:

- Personal data of any staff member of the organisation
- Any data pertaining to a client or customer of the organisation
- Any confidential company information which, if made public, would put at risk the Academy's reputation or jeopardise the commercial viability of the organisation.

7.1.2 Intellectual Property

Intellectual property owned by third parties, be they individuals or business entities, should not be inputted into any AI application. Staff and students should comply fully with the AI application's terms of use and should ensure the copyrighted data of any third party is not inputted without the explicit permission of the third party. Copyrighted data referring to any content that is legally protected under copyright law. If there is any confusion over what constitutes as copyrighted data, please consult with the Research and Ethics Committee before processing this data through AI.

7.1.3 Accuracy/Bias Assessment

Generative AI applications may have been trained using incorrect or out of date datasets. Any AI application has the potential to "hallucinate", i.e. create outputs that appear correct but are in fact inaccurate. There is also the risk that outputs produced may be biased. Therefore, it is crucially important that users apply critical thought to any outputs produced by an AI application and any information produced by an AI is validated through manual research for verification that it is true and usable information. No AI application should be used without human oversight. It is the responsibility of all staff and students to thoroughly review any outputs produced by an AI application before relying on them for work or study purposes. The use of AI does not preclude staff and students from fact checking all information they are sharing either internally within the company or externally. Staff and students are solely responsible for the data they share. The mere fact that AI was used to produce such data is not a reasonable defence for distributing inaccurate data.

7.1.4 Incident Reporting

Any potential security issues or data breach related to the use of an AI application should be reported immediately to the ICT Department.

7.1.5 Ethical and Responsible Use

Any use of an approved AI application should be done ethically and responsibly. Content should never be generated for the purposes of bullying or harassing any other individual. AI applications should not be used to generate content which is explicit or offensive.

7.1.6 Transparency

It is important that staff and students are transparent in their use of AI systems. While AI may be used to assist staff and students in their work and study, the use of AI should be openly acknowledged and no outputs produced by AI should be claimed as the user's own work.

It is required that any piece of work that was created with the assistance of AI, includes a statement of transparency detailing that this work was assisted by AI in accordance with the RIAM AI Governance Policy

7.1.7 Environmental Impact

The use of AI requires significant computational power, which could contribute to energy consumption and carbon emissions. RIAM encourages users to use AI tools responsibly and be mindful of their environmental footprint, choosing alternative, more eco-friendly tools where possible and endeavouring to only use AI when necessary. RIAM supports sustainable AI practices and will continuously monitor AI's ecological impact and update their practices when necessary.

8. Unacceptable AI Usage Guidelines

8.1 To ensure integrity and clarity across the organisation, the use of AI at RIAM by both personnel and students will never be used in the following manner:

Students:

Students should never use AI in the following manner:

- to generate entire assignments, essays, research papers, or any work submitted as their own, original, material
- to engage in plagiarism by copying AI-generated content without citation.
- to complete exams, quizzes, or assessments unless explicitly permitted by the instructor.
- to fabricate data, references, or misinformation in academic submissions.
- to generate misleading, unethical, or harmful content

Students should never use AI-powered tools while taking the following assessments:

- In-person unseen examinations
- Class tests
- Some online tests
- Viva Voces
- Some laboratories and practicals
- Discussion-based assessments
- Where spoken and written language skills need to be assessed.

Teaching & Administration Staff :

- Under no circumstances are Gen AI tools to be used to share private personal or sensitive data, such use is unlawful. This includes entering such data in a search prompt to an AI tool.
- Certain types of information must never be provided to an AI tool hosted outside RIAM including:
  - Passwords and usernames
  - Personally identifiable information (PII) or other sensitive or confidential material, irrespective of any perceived lawful basis, including explicit consent
  - Any data that has not been properly anonymised to ensure it is non-identifiable
  - Any data that is not fully consistent with RIAM's policy on Data Protection
  - Any data related to RIAM Intellectual Property
  - Any data that is protected by Copyright
  - Any prompts or data, whose responses might result in reputational damage to RIAM.
  - Any non-PII data from third parties where the individual has not explicitly consented for their data to be used with AI, with the exception of data that is clearly already in the public domain.
- Confidential material must not be submitted as search prompts for GenAI tools
- Staff who suspect material submitted to them has been generated by AI-powered tools should not use AI detection tools. This is because:
  - currently these tools are insufficiently accurate for RIAM to use them as evidence
  - submission of the work to such tools may represent a data security breach
  - the document being checked becomes available as training data for other AI tools
- AI-powered tools should not be used autonomously for grading assignments / examinations or for critical decision-making (admissions, grading, disciplinary actions).

9. Acceptable AI Usage Guidelines

For Students:

As a general principle, students may use generative AI to help them learn but they may not use AI to generate or falsify work.

Students may use Gen AI in ways that support their learning, enhance their ability to achieve their learning outcomes, and prepare them to succeed in their future careers.

However, using Gen AI to falsify work or breach guidelines for an assessment will undermine all these benefits and damage their learning.

Students should always make sure that the Academic Integrity principles are followed in any work that they do, and when in doubt, always ask their teachers about the appropriate use of Gen AI.

- Users should check the assessment brief or have spoken with their teacher or supervisor to confirm that the use of Gen AI is not prohibited for their assessment type.
- Students should review the Academic Integrity principles to help avoid unintentional plagiarism.
- Students should review the risks and limitations of using Gen AI including a recognition of issues of bias, sensitivity, accuracy, appropriate consent and ethical issues
- Students should critically evaluate any AI tools they use, consider how the tools will use the data they input and chose the appropriate tools for the task they are completing, cross checking that these tools are included within the Academy's usage list before using them.
- Students should fact-check any output AI-powered tools produce.

- Students should critically review all quotations, or citations or outputs that the Gen AI tool has generated and thoroughly verify same.
- Students should check that they have not submitted any personally identifiable information (PII) to a Gen AI tool.
- The use of the AI-powered tools must be adequately documented so that they can be appropriately acknowledged.
- Users should check the latest editions of Chicago Style or APA manuals for guidance on appropriate referencing. Additional guidance is provided by RIAM's Guide to Chicago Style on Moodle VLE.
- Students should ensure that their assignments and research remain their own work.
- Students should retain copies of Gen AI outputs used in the preparation of assignments.
- Students should keep drafts of their work so that they can evidence the process they used end-to-end. This should include all prompts submitted to generate content.
- Students may be asked to provide these copies as appendices to their assignments or as part of any misconduct process.

For Teaching & Administration Staff:

- Staff should ensure that their use of AI is ethical and within RIAM's regulations
- Staff should be transparent about their own use of Gen AI tools in their work.
- Submission of copyright content as prompts to Gen AI tools should be within Fair Dealing guidelines.
- All material that is wholly or substantially generated using an AI tool should be declared clearly in the document in which it occurs, whether the document is for internal or external use.
- Staff engaged in the development or use of AI in any type of learning activity should ensure that the AI-based learning activity is ethical and conforms to RIAM's regulations.
- Staff engaged in the development or use of AI in any type of research should ensure that the AI usage is ethical and conforms to RIAM's regulations, including where appropriate and necessary by obtaining authorisation from a faculty research ethics committee.
- The presentation of work (e.g. for conferences, publications, presentations) that has used AI should be carried out in accordance with the guidelines and regulations on the use of AI supplied by the research funder, conference organiser or publisher, as well as those of RIAM.
- Staff with supervisory responsibilities (either academic or managerial) should ensure that those working with them are aware of the College's guidance on the use of AI.
- Lecturers instructing their students to consider AI tools should provide the students with guidance as to acceptable use, particularly regarding plagiarism, data protection, sensitive information and critical evaluation of results.

10. Responsibility

10.1 RIAM will comply with its legal responsibilities under the EU Artificial Intelligence Act and provide training in the responsible use of AI to staff members and students.

10.2 The Secretary is responsible for ensuring that staff and students follow this policy and adhere to all related procedures.

10.3 Periodic reviews of the measures and practices in place shall be carried out.

11. Legislation and Regulation

11.1 European Union Artificial Intelligence Act
11.2 Assessment List for Trustworthy Artificial Intelligence (ALTAI)
11.3 General Data Protection Regulation (GDPR) (EU Regulation 2016/679)
11.4 General Data Protection Act 2018
11.5 Data Protection Commission Breach Notification

12. Related Documents

12.1 RIAM Data Protection Policy
12.2 RIAM ICT Policy
12.3 RIAM Privacy Policy
12.4 Data Breach Management Policy

13. Review

13.1 Due to the continually evolving nature of AI scope and the global landscape, this policy will be subject to constant monitoring and will be reviewed on a quarterly basis, or as required to take into account changes in the law.

14. Document Control

Approved by Governance and Nominations Committee: 23rd June 2025

Approved by RIAM Governing Body: 10th July 2025

This policy will be reviewed on a quarterly basis, or as required to take into account changes in the law.