Dukes Education
AI Governance, Policy, and Implementation

1. Overview

The Lyceum believes that Artificial Intelligence (AI) has the potential to enhance our human capacity. AI creates a myriad of opportunities for schools and is an exciting opportunity to explore the fundamentals of learning. We will harness AI's potential to enhance teaching innovation whilst ensuring the safeguarding and protection of our students remain at the heart of what we do. With this as our mission, The Lyceum is committed to integrating AI in a responsible, ethical, and legally compliant manner. Its deployment in schools requires rigorous safeguards to protect student and staff privacy, ensure fairness, and maintain transparency.

This policy establishes the regulatory, ethical, and operational framework for AI use across the Dukes Education family, ensuring alignment with the EU AI Act, GDPR, anti-discrimination laws, cybersecurity standards, and child protection regulations.

2. Purpose and Scope

2.1 Purpose
This policy provides a structured approach to the responsible and innovative adoption and use of AI technologies, ensuring compliance with evolving legal and ethical standards while fostering innovation in education.

2.2 Scope
This policy applies to:

- All staff, educators, and administrators at The Lyceum.
- All pupils and parents/guardians interacting with AI-based systems in school.
- Third-party vendors and service providers engaged in AI-related technology procurement must adhere to institutional guidelines. Please consult the vendor guidelines for more detailed information.
- Any AI-driven smart technology used within the institution, including but not limited to generative AI, predictive analytics, smart glasses, virtual reality (VR), and adaptive learning systems.

3. Legal and Regulatory Compliance

AI regulations vary by country and evolve rapidly. The Lyceum commits to full compliance with:

- The EU AI Act (where applicable): Mandating risk-based regulation, prohibiting harmful AI uses, and imposing strict transparency and accountability measures. AI systems will be classified according to their risk level, with high-risk systems subject to more stringent requirements. This includes systems used for vocational training and selection for further/higher education, which may be classified as high-risk due to their potential impact on individuals' life opportunities.
- The General Data Protection Regulation (GDPR): Ensuring AI systems respect privacy principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and user rights (access, rectification, erasure, restriction, data portability, and objection).

- National and Local Anti-Discrimination Laws: Ensuring AI applications do not introduce, perpetuate, or reinforce bias based on gender, race, disability, socio-economic status, or any other protected characteristic.
- Child Protection Regulations: Ensuring that all AI systems are designed and used in a way that protects the safety, wellbeing, and rights of children. In the UK, this includes compliance with KCSIE 2025 and the DFE Guidance (https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education#further-information).
- Examination Board Academic Integrity Guidelines: Ensuring that the use of AI supports and does not undermine academic integrity.

All AI-driven technologies used at The Lyceum must undergo pre-deployment risk assessments, ensuring they do not infringe on pupils' rights, academic integrity, or child protection laws.

STAFF ARE PROHIBITED FROM INDEPENDENTLY SETTING UP AI ACCOUNTS WITH THEIR WORK EMAIL ADDRESSES OR USING UNAUTHORISED AI TOOLS IN CLASSROOMS. ALL AI-DRIVEN TECHNOLOGY USED IN SCHOOL MUST BE INSTITUTION-APPROVED AND MEET STRICT COMPLIANCE AND SECURITY STANDARDS.

4. Policy

4.1 Data Privacy and Security

The Lyceum prioritises data privacy and adheres to GDPR and cybersecurity best practices. To protect student and staff data, all AI systems must:

- Comply with GDPR & Legal Regulations: AI tools must process and store data in compliance with GDPR and other applicable data protection laws. AI vendors must provide clear data privacy policies before implementation in schools
- Limit Data Collection & Storage: AI tools should only collect the minimum necessary data to function. Pupil and staff personally identifiable information (PII) must not be stored or shared without consent.
- Never collect, store, or process highly sensitive student data (e.g., biometric, behavioural, or health information) unless explicit legal and parental consent has been obtained.
- Use strong encryption to safeguard data from unauthorised access, hacking, or breaches. This means that all stored or transmitted data must be secured using industry-standard encryption protocols to prevent misuse.
- Monitor and Audit AI Data Usage: Schools must regularly review and audit AI systems to detect potential data breaches or misuse. A Data Protection Officer (DPO) should oversee AI compliance and risk management.
- Obtain Explicit Consent for AI Use: Schools must obtain consent from students, parents, or staff before using AI systems that process personal data.
- Protect AI Systems from Cyber Threats: AI platforms must be secured against hacking, unauthorized access, and data leaks. Schools should conduct regular cybersecurity assessments of AI tools used in classrooms.
- Apply pseudonymisation and anonymisation when handling personal data, ensuring that identifiable information is removed or replaced to protect individuals' privacy.
- Give users the right to opt out of AI-based profiling and automated decision-making processes where legally required, ensuring that students, staff, and families retain control over their personal data.

4.2 Ethical AI Use

All AI tools must adhere to fairness, accountability, and transparency principles in line with the EU AI Act, UNESCO AI Policy Makers Guidance and UK Department of Education:

- Bias Prevention: AI tools must be audited regularly to detect, prevent, and eliminate biases in recommendations, grading, or any other outputs. This includes ongoing monitoring and evaluation of AI systems for fairness and non-discrimination.
- Pupils, parents, and staff must have clear mechanisms to challenge AI-based decisions and receive timely and meaningful explanations for such decisions.
- The use of AI tools in educational processes and decisions should be transparent to all stakeholders.
- To the extent technically feasible, AI systems should be designed to provide explanations for their outputs, promoting understanding and trust.
- Human Oversight: AI must not make final decisions on admissions, student grading, disciplinary action, or staff evaluations. Human review is mandatory for all significant decisions informed by AI.

The 'human in the loop' framework is applied when:

- Deciding which AI tools to use.
- Preparing resources.
- Supporting learning.

The Head of Computing & STEAM is the key authority when assessing the impact of AI. They must:

- Assert their agency over the technology.
- Evaluate if AI is having a positive impact.
- Ensure that AI does not replace one-to-one support.
- Ensure users are not becoming overly reliant on AI.

4.3 Accessibility and Inclusion

AI should be inclusive and enhance learning for all students, including those with disabilities or diverse linguistic backgrounds. Schools must:

- Ensure all AI-driven platforms comply with accessibility standards (e.g., WCAG international guidelines).
- Prioritise multilingual AI tools to support equity in access for non-native speakers.
- Use AI to provide assistive technologies (e.g., AI captioning, dyslexia-friendly interfaces).

4.4 AI in Smart Wearables & VR

AI-driven smart glasses, VR, and AR (augmented reality), and other wearable tools must:

- Be pre-approved by The Lyceum before use.
- Never record, store, or share pupil AI interactions without explicit pupil and guardian consent.
- Have privacy controls in the software settings ensuring that student data is processed lawfully.
- Be monitored to prevent misuse (e.g., facial recognition, behaviour tracking).
- Never be brought into areas requiring additional sensitivity, such as bathrooms, changing rooms, medical or health support areas, and other designated private spaces where the use of image, video, or audio-capturing technology would violate privacy and safeguarding policies.

Unauthorised AI-driven wearables and VR applications must not be used in any school environments by any staff, students, or visitors.

4.5 AI Procurement & Vendor Requirements

All AI vendors must:

- Pass a Vendor Risk Assessment, ensuring compliance with AI ethics, cybersecurity, and legal standards.
- Use encryption (at rest and in transit) to protect sensitive student and school data.
- Implement strict access control measures to prevent unauthorized use.
- Ensure AI tools do not retain or misuse user data beyond contractual terms.
- Offer regular security updates to address vulnerabilities
- Vendors must provide clear accountability structures for AI failures or risks, such as documented risk assessments.
- Ensure a human oversight mechanism for critical AI decisions.
- Establish protocols for handling AI-related errors and unintended consequences
- Vendors must have documented risk mitigation policies and clear processes for addressing AI-driven errors affecting students or staff.
- Vendors must provide comprehensive training materials for educators and administrators.
- Ensure dedicated support for troubleshooting and updates, at least for enterprise or paid plans, while providing essential support documentation for all users.
- Vendors must provide AI literacy resources, which may include structured training programs, webinars, or other learning opportunities to help users understand AI tool limitations.
- Vendors must commit to ongoing improvements in AI ethics, accuracy, and compliance.
- Vendors must provide channels for educators and administrators to submit feedback on AI performance and implement a process for continuous improvement.
- Vendors must disclose the AI models used, their data sources including AI stack composition, and the bias mitigation strategies implemented to prevent hidden biases.
- Provide explainability, ensuring staff, educators, pupils, and families understand how AI-generated outputs are produced.
- Agree to annual audits to maintain compliance.

Please consult the vendor guidelines for more detailed information.

4.6 Sustainability

Generative AI uses large amounts of energy to train models and to create media. There is an environmental impact to consider, therefore its use must be purposeful and used only when necessary.
AI tools should be designed and deployed with minimal environmental impact:
Energy-Efficient AI Models

- Prioritize vendors that use low-energy AI models to reduce carbon footprints.
- Choose cloud-based AI services

Sustainable Infrastructure

- Use AI systems that optimize data storage and computing power.
- Implement server cooling and eco-friendly hardware solutions.

5. Staff Use of AI

Under the EU AI Act, staff must adhere to strict regulations governing the use of AI in educational settings. The following actions are strictly prohibited:

- Processing or inputting sensitive personal data into AI systems – Staff must never enter or share pupil, staff, or institutional data (including academic records, health data, or financial information) within AI platforms, unless explicitly authorised and in full compliance with GDPR and data protection regulations.
- Using AI for fully automated decision-making in areas that significantly impact students or staff – AI must not be used to make final decisions regarding admissions, grading, disciplinary actions, or staff evaluations without human oversight and intervention.
- Deploying AI tools that lack transparency or accountability – Any AI system used within the institution must be explainable, meaning educators and administrators must understand how AI-generated decisions are made and be able to justify their use.
- Allowing AI to introduce bias in educational practices – Staff must ensure that AI tools do not discriminate based on gender, race, disability, or socio-economic status. Any detected bias must be reported and addressed immediately.
- Using unauthorised AI tools or personal AI accounts – All AI technologies must be institution-approved. Staff must never create personal accounts on external AI platforms for school-related tasks. All tools, after being approved by the school, must be tested extensively in a sandbox environment. Tools are then categorised according to acceptable uses. This must happen before deploying them with students or inputting sensitive data.
- Recording, tracking, or analysing pupils' behaviour through AI-driven monitoring systems without explicit consent – AI-based surveillance, facial recognition, or emotion detection technologies are prohibited unless they comply with strict legal safeguards and receive formal approval.
- Failing to inform students and families when AI is being used – Transparency is essential. Staff must clearly communicate when and how AI tools are implemented in teaching, learning, or administrative processes.
- AI-Generated Pupil Feedback Without Human Review: AI cannot provide personalized feedback to students without human verification.

6. Governance and Accountability

Responsibility and Accountability Framework

To ensure clear governance, transparency, and compliance, the following table defines the responsibility and accountability structure for AI use across all levels of the organization. Responsibilities are assigned at the Group, Regional, School, IT/Data Protection, and Individual Staff levels to promote consistent implementation, safeguard data privacy, and uphold ethical standards in all AI-related activities.

Level	Responsibility	Examples
Group (e.g. Dukes' Education Board)	Set strategic AI governance policies, ensure compliance across all schools, conduct group-wide risk oversight.	- Approving AI Governance Policy - Conducting strategic audits - Updating policies based on EU AI Act changes

Regional Leadership (e.g., European, UK Leaders)	Adapt group policies to regional and legal requirements, ensure regional schools implement accordingly.	- Adjusting policy to match local GDPR or national AI laws - Providing regional compliance reports.
School Leadership (Head/Principal, Senior Leadership Team)	Implement policy locally, approve AI tools for use in school, train staff, monitor compliance.	- Approving AI tools for teaching - Ensuring staff complete AI compliance training - Responding to incidents or breaches
IT & Data Protection Teams	Ensure AI tools meet cyber security and GDPR standards; monitor technical risks; advise on safe deployment.	- Conducting vendor risk assessments - Managing data security audits - Advising on pseudonymisation/anonymisation
Individual Staff (Educators, Administrators)	Use AI responsibly according to policy, seek approval before using new tools, protect personal data.	- Using only approved AI systems - Not creating unauthorized AI accounts - Reporting concerns about AI tools
Vendors	Meet contractual requirements for ethics, privacy, security, and compliance, support audits and provide explainability.	- Providing secure and ethical AI tools - Submitting to annual compliance reviews - Supporting AI literacy training for users

6.1 Ultimate Responsibility

The Head/Principal of School is accountable for ensuring the implementation, compliance, and enforcement of this AI Governance Policy within their school.

Strategic oversight and risk management rest with the Board of Governors or Trustees, ensuring that AI use aligns with ethical, legal, and educational standards.

The Dukes UK Board holds overarching responsibility for ensuring that all schools within the group comply with this policy and all applicable regulations.

6.2 Governance Structure and Responsibilities

- Head of School / Principal: Accountable for ensuring all staff, pupils, and AI applications comply with institutional, national, and EU AI regulations.

- School Governing Body: Responsible for oversight, risk assessments, compliance monitoring, and policy updates in line with technological and legal advancements.
- IT and Data Protection Teams: Ensure that AI tools meet cybersecurity, GDPR, and student data protection standards.
- The Data Protection Officer/Bursar and Head of Operations will be responsible for:
    - Understanding and maintaining awareness of what the use of AI means for data protection in the school.
    - Advising the school on how to integrate the use of AI while complying with data protection regulations.
- ICT support will be responsible for:
    - Providing technical support in the development and implementation of the school's AI practices, policies and procedures.
    - Implementing appropriate security measures.
    - Ensuring that staff receive regular, up-to-date training on how to use AI tools in school
- All staff members:
    - Adhering to the Acceptable Use Agreement and other relevant policies.
    - Taking responsibility for the security of the AI tools and data, they use or have access to.
    - Modelling good online behaviours when using AI tools.
    - Maintaining a professional level of conduct in their use of AI tools.
    - Having an awareness of the risks that using AI tools in school poses.
    - Reporting concerns in line with the school's reporting procedure.
    - Where relevant to their role, ensuring that the safe and effective use of AI tools is embedded in their teaching of the curriculum.
    - Familiarising themselves with any AI tools used by the school and the risks they pose.

- Senior Leadership Team (SLT): Supports staff training, policy communication, and ongoing evaluation of AI-driven technologies.
- Pupil & Parent Advisory Group: Provide feedback on AI's impact on education and learning outcomes. Advocate for fair AI policies that protect student rights. Ensure AI tools respect student privacy & prevent biases. Raise concerns about AI-related ethical or security issues.

7. Review & Compliance

7.1 Semi-Annual Policy Review

This policy is a live document and will be reviewed twice per year (semi-annually) to ensure ongoing alignment with:

- Advancements in AI technology.
- EU AI Act – Ensuring AI governance aligns with evolving European regulations
- GDPR Compliance – Protecting student and staff data privacy.
- Changes in EU, national, and global AI regulations.
- Evolving best practices in AI ethics and safety.
- Feedback from staff, educators, students, families, and AI oversight committees.
- Institutional & Operational Needs

7.2 Non-Compliance

Failure to comply with this policy may result in disciplinary action and, where applicable, legal consequences.

For inquiries, contact The Lyceum

Written by Dukes' Education: August 2025

Updated by MS: September 2025

Next review: January 2026