



msletb

Bord Oideachais agus Oiliúna
Mhaigh Eo, Shligigh agus Liatroma
Mayo, Sligo and Leitrim
Education and Training Board

Mayo, Sligo and Leitrim Education and Training Board

AI SECURITY POLICY

MSLETB,
Newtown,
Castlebar,
Co. Mayo
F23 DV78

V1

DOCUMENT CONTROL SHEET

Business Unit	ICT Department, MSLETB
Work Category	ICT
Document Title	AI Security Policy
Document No.	V1

Rev (per footer)	Status	Author(s)	Reviewed By	Approved By	Office of Origin	Issue Date
V1	Approved	ICT, DP	SM, SC, BB, SF, CL & OR.	EMT 10/09/2024 Noted by the Board of MSLETB on 24/09/2024	HQ Castlebar	24/09/2024

Contents

1	Policy Statement	1
2	Scope.....	1
3	Definitions.....	2
4	Policy Review, Approval and Continuous Improvement	2
5	Objective	2
6	Risks of AI	3
7	User Responsibilities	4
8	Acceptable AI Usage Guidelines.....	5
9	Unacceptable AI Usage Guidelines	5
10	Enforcement.....	6
11	Related Policies	7

1 Policy Statement

The purpose of this AI Policy is to ensure the ethical, responsible, and transparent use of Artificial Intelligence (AI) within Mayo, Sligo and Leitrim Education and Training Board (hereafter referred to as 'MSLETB'). MSLETB are committed to harnessing the power of Artificial Intelligence (AI) to enhance learning and teaching while upholding the values of academic integrity and responsible use. MSLETB acknowledges the potential risks associated with the use of Artificial Intelligence (AI) tools. As a result, MSLETB are dedicated to ensuring the confidentiality, integrity, and accessibility of all organisation users and student data. This policy mandates that all users employ AI tools in alignment with our established security best practices.

2 Scope

This policy applies to all approved "Users" of MSLETB's systems, information and I.T. resources. Individuals covered by the policy include but are not limited to employees (both full and part time), contractors, interns, partners and / or consultants, external individuals, and organisations here on in to be referred to as "Users".

Please note, by logging on to and/or using any organisation IT resource whether directly or by remote access or by other means, including using non-Organisation resources to access organisation data or systems, all parties shall be deemed to have agreed to be bound by the terms of this Policy.

3 Definitions

Personal Data	Personal data means any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Confidentiality	Confidentiality restricts information access to authorised users.
Integrity	Integrity protects the accuracy and completeness of information through the controlling of information modifications.
Availability	Availability ensures the information is accessible when needed.
Artificial Intelligence or AI	AI, or Artificial Intelligence, refers to the development of computer systems that can perform tasks and make decisions that typically require human intelligence. It involves creating algorithms and models that enable machines to learn from data, recognize patterns, and adapt to new information or situations.
Teaching with AI	The integration and utilization of AI tools in teaching methodologies, instructional design, and student assessment to enhance learning outcomes.

4 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, who are committed to continually improving the protection of all MSLETB information assets and the protection of personal data where MSLETB is a controller or processor. This document will be reviewed at least every 1 year by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within MSLETB.

5 Objective

The aim of this policy is to ensure that every user utilises AI tools with a focus on security, responsibility, and confidentiality. It delineates the obligations users must adhere to when employing AI tools, including the assessment of security risks and the safeguarding of confidential data.

6 Risks of AI

The use of AI tools presents risks to both users and the organisation.

Users of AI tools must accept risks and consequences involved in use of AI in development of documentation, projects, or publications that they develop through the use of the available AI technology, including but not limited to:

1. Privacy Breaches
2. Bias and Fairness
3. Lack of Accountability (potentially provides false or incorrect information)
4. Security Threats
5. Ethical Concerns
6. Excessive reliance and overdependency on AI

7 User Responsibilities

All users are expected to adhere to the following when using AI tools:

a. Evaluation of AI tools: Prior to deployment of an AI Tool a Data Protection Impact Assessment (DPIA) must be provided to the DPO to assess the security aspects of any such AI tool. This entails reviewing the tool's security features, terms of service, and privacy policy. Additionally, the DPIA should scrutinize the reputation of the tool developer and any third-party services integrated into the tool. AI tools or AI software must not be used without prior approval from IT and DPO.

A DPIA should be submitted to DPO via email to dataprotection@msletb.ie.

b. Protection of confidential data: Without prior authorisation from the relevant department, users are prohibited from uploading or sharing any data considered confidential, proprietary, or protected by regulatory standards. This includes data pertaining to students, learners, staff, board members, customers, users, or MSLETB business.

c. Access Control: Users must not grant access to AI tools to external parties without prior consent from the ICT / Data Protection department, following the necessary procedures to meet security compliance requirements. This encompasses refraining from sharing login credentials or sensitive information with third parties.

Users must apply the same procedures/protocols outlined in MSLETB's Access Control Policy.

d. Use of reputable AI tools: Users are to exclusively employ trustworthy AI tool(s) and are prohibited from using tools developed by individuals or entities lacking established reputations. All AI tools require approval from IT and DPO.

e. Compliance with security policies: Users must apply the same security procedures/protocols as outlined in our IT and Data Protection policies. This includes the utilization of robust passwords, maintaining software currency, and adherence to our data retention and disposal policies.

f. Data privacy: Prior to uploading or sharing data into AI tools, users should exercise discretion regarding public disclosure. Users should ask themselves, "Am I comfortable with this information being disclosed beyond the organisation? Is public disclosure acceptable?" This process should align with the principles outlined in (b) above.

8 Acceptable AI Usage Guidelines

1. Ethical Considerations

Users of Artificial Intelligence at MSLETB must ensure that the generated content used does not in any way promote hate speech, discrimination, harassment, or any other form of harmful or offensive material.

2. Information Verification and Fact Checking

Users should carefully review AI generated material before use. Users are responsible for ensuring AI generated material is accurate, relevant, and appropriate.

3. Transparency and Attribution

Users should communicate openly and clearly about the use of AI technologies in the organisation, ensuring that staff, students, and third parties have a comprehensive understanding of their purpose, capabilities, and potential impacts.

4. Accessibility

Users employing AI to generate training materials should consider accessibility requirements, so the material is accessible to all staff, students, and third parties.

5. Accountability

The organisation will actively engage all users in the decision-making processes related to AI usage. Open channels of communication and feedback mechanisms will be established to foster transparency and inclusivity.

9 Unacceptable AI Usage Guidelines

To ensure integrity and clarity across the organisation, the use of AI at MSLETB should never be used in the following manner:

1. To plagiarise or use another person's or organisation intellectual content without original creator's permission/ reference to the materials used. Users should not use AI tools to create or submit work without proper attribution or authorisation.
2. To harass, bully, intimidate, or discriminate against other users or external parties.
3. To create any content that is illegal, discriminatory, defamatory, or otherwise offensive or inappropriate to any users or third parties.
4. To share personal data, confidential, or sensitive organisational information with unauthorised users, including external parties that provide AI services.
5. To engage in any activity that could compromise the security or integrity of the organisation using AI systems, including allowing tool access to provisioned laptop, device, network, unauthorised data sets and systems.
6. To violate any applicable laws or regulations, including data protection, intellectual property, privacy laws or geographical restrictions by using data within AI without prior consent, approval or permission of data owners.

10 Enforcement

All users of MSLETB's ICT Department systems, information and I.T. resources have a responsibility to promptly report any known instances of non-compliance to management or MSLETB's ICT Department.

Compliance

Individuals found to be in breach of this policy, may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

All users will be required to undertake ongoing ICT and GDPR awareness training.

If a breach of personal data occurs, then this must be reported to MSLETB's Data Protection Officer by emailing dataprotection@msletb.ie.

11 Related Policies

- MSLETB Data Processing Policy
- MSLETB ICT Acceptable Usage Policy
- MSLETB Data Retention Schedule
- MSLETB Internet Acceptable Usage Policy
- MSLETB Encryption Policy
- MSLETB Virus Malware Protection Policy
- MSLETB ICT Framework Policy
- Department of Education and Skills circular on Revised Procedures for Suspension and Dismissal of Teachers and Principals (ETBs).
- ETBI & Unions Consultative Forum - Disciplinary Procedure for staff employed by Education & Training Boards.
- Procedures for principals relating to their work, conduct and matters of professional competence in their role as principals