Table of Contents

1. Purpose and Scope 3
2. Ethical Use and Bias Prevention 3
3. Legislation and Guidance 4
4. Definitions 5
5. Acceptable use of AI 5
6. Prohibited Practices & Prohibited Use of AI 6
6.1 Prohibited AI Practices 6
6.2 Prohibited Use of AI 7
7. Training 7
8. Roles & Responsibilities relating to this policy 8
8.1 User Responsibilities 8
8.2 Management Responsibilities 9
8.3 ICT Responsibilities 10
8.4 Data Protection Officer responsibilities 10
9. AI Adoption Process 11
10. Monitoring & Auditing 13
11. Risk Management 13
12. Human Oversight 13
13. Mandatory Disclosure 13
14. Transparency 14
15. Environmental Considerations 14
16. Data Protection and Security 14
17. Incident Reporting 15
18. Other Relevant Policies & Documents 15
19. Enforcement 15
20. Review of this Policy 15
20.1 Revision History 16
20.2 Distribution Record 16

Appendix 1. Responsible AI usage for Public Service 17
Appendix 2. Guidelines for Ethical AI Usage in DDLETB (Do'd & Don'ts) 18

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

1. Purpose and Scope

DDLETB recognises the potential of Artificial Intelligence (AI) to enhance educational delivery, administrative efficiency, data-informed decision-making, and organisational innovation. This policy aims to support the responsible, ethical, and secure use of AI technologies across DDLETB services while ensuring compliance with legal, regulatory, and public-sector obligations.

This document sets out the fundamental principles, responsibilities, and governance structures for the use of AI within DDLETB. It provides for the ethical, secure, and transparent adoption of AI technologies by DDLETB employees ensuring alignment with legal obligations under the EU AI Act and other relevant frameworks.

This Policy covers not only any GenAI products that DDLETB provides to its employees, but also any third party or publicly available GenAI tool such as ChatGPT, Gemini, CoPilot and any other applications that mimic human intelligence to generate answers or perform certain tasks that are used by DDLETB's employees in a professional activity.

This Policy outlines acceptable uses, approval processes, and safeguards to protect data integrity, organisational reputation, and the wellbeing of learners/students and staff.

This Policy also refers to various supporting material such as the AI Policy Guidance Document which should be read in conjunction with this Policy to ensure full understanding of the accepted process for engaging with AI within DDLETB

This Policy is relevant to all staff employed by DDLETB, and relates to the use of AI, for example generative, agentic, analytic, and all its currently known outputs, text, audio, image, video. All AI is to be recorded in the AI Adoption Register which may expand to include new AI technology and outputs upon review by senior management.

2. Ethical Use and Bias Prevention

It is the position of DDLETB that the value of AI should not be realised at the cost of quality and value to either the ETB or the people it serves, DDLETB will strive to ensure that the use of any AI is considered from a "Human first" perspective, using only AI that can show a proven track record of legal adherence and respect for the source of any materials used to train itself.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

DDLETB will carry out appropriate due diligence to proactively detect inherent bias both prior to deployment and post deployment to ensure that there are no unwarranted or unexpected outcomes. According to the 'Guidelines for the Responsible use of AI in the Public Service', algorithmic bias can be caused by the use of training data that reflects the existing systemic biases or by not being representative of the population that will use the AI. As a result, DDLETB will take particular care to ensure that vulnerable groups are not adversely affected. DDLETB will ensure proper oversight is provided so that the AI model itself is ethically balanced.

DDLETB is aligned with the seven principles for the responsible use of AI as a public body as set out in the government issued Guidelines for the Responsible Use of AI in the Public Service, (Guidelines_for_the_Responsible_Use_of_AI_in_the_Public_Service.pdf) *i.e.* (1) Human agency and oversight, (2) Technical robustness and safety, (3) Privacy and data governance, (4) Transparency, (5) Diversity, non-discrimination, and fairness, (6) Societal and environmental well-being and (7) Accountability.

Appendix 2 of the Policy sets out the Guidelines for Ethical AI Usage in DDLETB *i.e.* a list of do's and don'ts.

3. Legislation and Guidance

The following are relevant legislation and guidance:

- Regulation (EU) 2024/1689 ('AI Act')
- General Data Protection Regulation 2016/679
- Data Protection Act 2018 (as amended)
- 'Guidelines for the Responsible Use of Artificial Intelligence in the Public Service' – Department of Public Expenditure NDP Delivery and Reform.

Please note that records created by AI are also subject to the Freedom of Information Act 2014 (as amended).

4. Definitions

'AI Act' refers to Regulation (EU) 2024/1689 which is legislation enacted by the European Union to ensure that AI systems are used in a safe, transparent manner that is aligned with fundamental human rights. It categorises AI systems by risk levels and sets compliance principles accordingly.

'**Artificial Intelligence (AI) system'** means *"…' a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;*

'Encryption' is the process of converting information so that it cannot be read by unauthorised people;

'Generative AI' ('GenAI') is a type of AI that is designed to generate content, such as text, images, or code, based on input data. Examples of GenAI are chatbots and ChatGPT.

'User' refers to an employee, whether full or part time, contractor, intern, partner, consultant, external individual or organisation.

5. Acceptable Use of AI

The ETB will ensure that its employees review the AI Adoption Register prior to using AI to ensure that such system is on the list as having been approved for use by DDLETB. This register will provide direction on the type of data that can be used within a specific tool and whether or not its use needs to be disclosed, *etc*. When using AI, Users must follow the requirements set out in this Policy and be cognisant of their responsibilities herein.

6. Prohibited Practices & Prohibited use of AI

Use of AI that is not listed as approved in the AI Adoption Register is prohibited.

AI systems that threaten people's safety, rights, or livelihoods are strictly prohibited (except in limited circumstances) as set out in 6.1 below.

6.1 Prohibited AI Practices

AI systems that do the following are prohibited:

6.1.1. Exploit vulnerable persons, manipulate and use subliminal techniques.
6.1.2. Use social scoring for public and private purposes.
6.1.3. Predict whether a person will commit an offence based solely on profiling that person (except where the AI systems is used to support the human assessment of the involvement of a person in criminal activity that is already based on objective and verifiable facts directly linked to criminal activity).
6.1.4. Use untargeted gathering of facial images from the internet or CCTV so as to build up or expand databases.
6.1.5. Use emotion recognition in the workplace and education institution, unless for medical or safety reasons.
6.1.6. Categorise people according to their biometric data to assume their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation (except where the labelling or filtering is of lawfully acquired biometric datasets, such as images, based on biometric data or categorising of biometric data in the area of law enforcement).
6.1.7. Use real-time remote biometric identification in publicly accessible areas and are used by law enforcement. This is subject to some limited exceptions.

6.2 Prohibited use of AI

The following items are a non-exhaustive list of behaviours in line with DDLETB's Code of Practice that are not permitted:

6.2.1. Use AI 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.
6.2.2. Use AI to harass, bully, intimidate, or discriminate against other users or external parties.
6.2.3. Use AI to create any content that is illegal, discriminatory, defamatory, or otherwise offensive or inappropriate to any users or third parties.
6.2.4. Use AI to engage in any activity that could compromise the security or integrity of the DDLETB, including allowing an AI access to provisioned laptop, device, network, unauthorised data sets and systems.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

6.2.5. Input of any personal, confidential, or sensitive ETB information into an AI system, unless explicitly sanctioned in the AI Adoption Register, and always with respect to the obligations to the GDPR.

7. Training

In accordance with Article 4 of the AI Act, DDLETB provides AI training to ensure, to their best extent, a sufficient level of AI literacy of its staff and other persons dealing with the operation and use of AI systems on its behalf. Users will be expected to fully engage with this training provided by DDLETB. If updated AI training is provided, Users are to avail of this training to ensure that they have a sufficient level of AI literacy when dealing with the operation and use of AI systems on behalf of DDLETB.

8. Roles & Responsibilities relating to the Policy

8.1 User responsibilities

A User must adhere to the following:

8.1.1. In the case of a suspected data breach within or as a result of use of an AI system, the User must contact their Line Manager immediately in accordance with the Data Breach Protocol. The Line Manager will contact the Data Protection Officer immediately and as per said protocol, the DPO will make an assessment of the incident and decide whether it is to be reported to the Data Protection Commission within 72 hours of the ETB becoming aware of the breach and/or whether it is to be reported to the data subject(s);

8.1.2. Adhere to this AI Policy, particularly section 6 above regarding Prohibited Use of AI;

8.1.3. Not engage with any AI without first reviewing the AI Adoption Register, in order to understand if it is accepted for use by DDLETB];

8.1.4. Complete AI literacy training as determined by DDLETB in accordance with the AI Act;

8.1.5. Follow the requirements mapped out in the AI Adoption Register when using AI. This register will provide direction on the type of Data that can be processed within a specific tool and whether or not its use needs to be disclosed, *etc.*;

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

8.1.6. Only use AI if necessary, due to its impact on the environment;
8.1.7. If using AI for autonomous decision making, ensure that it is always verified by a natural person, and aligned with DDLETB's Data Processing Policy;
8.1.8. Use critical thinking to evaluate any AI-generated outputs before relying on them for any purpose;
8.1.9. If the use of an AI, or a type of data is not noted in the AI Adoption Register, you may apply for the ETB to consider this new AI solution by following the AI Adoption Process set out at section 9.

8.2 OSD Management responsibilities

In addition to the User responsibilities above, a Manager/Director must adhere to the following:

8.2.1. For an AI system to be accepted for use, the AI adoption process set out in section 9 must be followed and sponsored by a suitable authority within the ETB before being reviewed by OSD for adoption and integration;
8.2.2. Provide training to ensure staff members are AI literate in accordance with the AI literacy obligations set out in Article 4 of the AI Act;
8.2.3. Any exceptions granted for use of AI in an otherwise restricted fashion, must be reviewed [every 6 months, in line with each academic term] and the authorisation of the sponsorship renewed.
8.2.4. The AI Adoption Register will be reviewed [annually] to assess the AI system's impact on administrative efficiency, value, and educational quality / outcomes for learners;
8.2.5. The ETB may block access to AI systems that are not listed as permitted in the AI Adoption Register;
8.2.6. Enable DDLETB to comply with its legal responsibilities under the AI Act and provide AI training to DDLETB employees;
8.2.7. Enable DDLETB to align its AI governance structure's roles and responsibilities with its information security management system processes;
8.2.8. Ensure that upon implementation of a new AI or expanded use of an existing AI, training will be made available by the sponsor directorate to ensure all relevant users are trained to use the AI as intended;

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

8.2.9. Be familiar with different risk levels of approved AI systems to understand the level of human oversight required and potential risks of such AI systems.

8.2.10. Ensure that DDLETB's AI systems are subject to an internal review every 6 months.

8.2.11. Ensure that DDLETB's AI systems are subject to review in response to questions or complaints raised by Users or other stakeholders. The results of such review and any remediation steps are to be recorded.

8.2.12. If AI systems are provided and managed by a third party, ensure that the third party's roles and responsibilities are carried out through effective oversight and contractual rights.

8.3 ICT responsibilities

In addition to the User responsibilities above, ICT must adhere to the following:

8.3.1. For an AI system to be accepted for use, the AI Adoption Process set out in this Policy must be followed and sponsored by a suitable authority within the ETB before being reviewed by OSD for adoption and integration;

8.3.2. Do not enable any AI system, without the [OSD / ISMS] team having completed a full review of the requested system;

8.3.3. Do not allow any exceptions to permitted data use without recording authorisation from the [system sponsor and DPO].

8.3.4. Do not enable access to any AI system without confirmed and recorded authorisation from the system sponsor which is in line with the ETBs current ISMS process;

8.3.5. Prior to an AI system being used by DDLETB, review the AI system's security features, terms of service and privacy policy;

8.3.6. Control access to all approved AI systems;

8.3.7. Restrict or revoke persons access to approved AI at any time for any purpose.

8.4 Data Protection Officer responsibilities

In addition to the User responsibilities above, the DPO must adhere to the following:

8.4.1. Ensure that DDLETB's Data Retention Schedule remains up to date regarding AI systems and records relating to AI systems;

8.4.2. Ensuring that DDLETB's Data Protection Policy is reflective of the data processing using the AI systems.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

9. AI Adoption Process

If an ETB user wishes to use an AI system / solution for a new purpose - that is not listed as acceptable in the AI Adoption Register - then prior to using such an AI solution, the ETB employee may submit a completed form (see Appendix 1) regarding such an AI solution.

An AI solution may be a new feature in an AI system that already exists, an AI system that was previously restricted or a new AI system that is not used by DDLETB

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

Step 2: Line Manager

- Review submission and assesses it's appropriateness for school/centre/campus.
- Agrees to support the request of the AI solution or refuses the proposal of the AI solution.
- If s/he decides to support the request of the AI solution, s/he must forward the request to their supporting Director for consideration.
- If s/he decides not to accept the request of the AI solution, s/he must inform the User of his/her decision and the reasons for that decision.

Step 1: User

- Review DDLETB AI Policy to see if the AI solution is prohibited.
- Check that the new AI solution is not already contained in the AI Adoption Register.
- Complete the Responsible AI Canvas Form] (Appendix 1).
- Submit the completed the Responsible AI Canvas Form (Appendix 1) to your Line Manager for consideration.

Step 3: Supporting Director

- Review submission and assesses it's appropriateness for adoption within the relevant directorate.
- If s/he is satisfied with the information and intended purpose and value of the AI system, s/he may decide to provide sponsorship for the adoption of the AI solution and support the request. S/He may then forward the request to the Director of OSD/ISMS for consideration.
- If s/he is not satisfied with the information and intended purpose and value of the AI system, s/he may refuse the request. In this case, the Supporting Director must inform the relevant Line Manager who forwarded the request of their decision and the reasons for the refusal.

Step 4: Director of OSD

- Consult with the ETBI Guidance Note, particularly the 'AI Use Decision Matrix'
- Request that the appropriate teams such as the ISMS team review the submission.
- Together with the appropriate teams determine the risk level of the proposed AI system and whether AI training would need to be updated if the request were approved.
- If s/he decides to approve the request of the AI solution, s/he will ensure that the relevant users receive updated AI training prior to using the AI solution if required and request that ICT update the AI Adoption Register accordingly. The Director of OSD once satisfied will issue instruction to integrate the AI Solution which may involve enabling a feature in a system that already exists, or allowing access to a solution previously restricted.
- If s/he decides to reject the request of the AI solution, s/he will inform the relevant Supporting Director who forwarded the request of their decision and the reasons for the refusal.

Step 5: ICT

- If the Director of OSD has approved the AI solution, ICT will implement the approved request accordingly, update the AI Adoption Register and consider whether the AI solution may require repeated sponsorship approval.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

10. Monitoring & Auditing

DDLETB's AI systems will be subject to an internal review every 6 months. DDLETB's AI systems may also be subject to external reviews.

DDLETB's AI systems will also be subject to review in response to questions or complaints raised by Users or other stakeholders. The results of such review and any remediation steps will be recorded.

11. Risk Management

DDLETB adopts the risk-based approach established by the European Union (EU) AI Act. All AI use cases must be classified into one of the four statutory risk tiers prior to procurement or deployment. DDLETB will evaluate risks related to bias, data misuse, and safety, applying mitigation strategies as needed. Where risks to fairness, equity, or accountability are deemed unacceptably high, DDLETB will choose not to implement AI solutions e.g. in areas such as admissions or assessments.

12. Human Oversight

If an ETB employee wishes to use an AI system that is not listed as permitted in the AI Adoption Register, then prior to using such an AI system, the ETB employee may submit a completed form (Appendix 1) for using such an AI system.

13. Mandatory Disclosure

If an ETB employee uses AI, s/he must check the AI Adoption Register to determine if s/he is required to disclose that s/he used AI as part of their work depending on the particular AI used. The AI Adoption Register will reflect that Users must disclose when content is generated by an AI system, particularly in communications, content generation, or interactions with the public or other stakeholders.

If the AI Adoption Register states that disclosure of the use of the relevant AI is mandatory, then any content created or summarised with the assistance of such AI should clearly state that AI was used and should not be presented as original work. For example, include a note such as:

> *"This document was created with the assistance of AI in accordance with DDLETB's Artificial Intelligence Policy."*

14. Transparency

An ETB must be transparent and open about the AI systems being used which includes notifying end users, such as students, learners, parents when they are interacting with an AI system such as a chatbots/AI agents/automated decision-makers. The ETB should ensure that more complex queries can be redirected to a human to answer. When the output has been generated by an AI system the user should refer to the AI Adoption Register to understand what level of transparency is required.

In accordance with the Guidelines for the Responsible Use of AI in the Public Service, an ETB must maintain clear documentation on AI model development which includes the data used, the processing that was carried out and algorithms used, the rationale for choices and for compromises made.

15. Environmental Considerations

The use of AI requires significant computational power, which will contribute to energy consumption and may increase carbon emissions. DDLETB 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.

16. Data Protection and Security

DDLETB 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 used by DDLETB except for those clearly set out in the AI Adoption Register. If there are exceptions to this prohibition for specific use cases, they will be noted and reviewed in the ETB's AI Adoption Register for all Users to understand.

Where possible, DDLETB should avail of security protocols when using AI systems *i.e.* encryption, access control and data anonymisation.

DDLETB prohibits the use of AI products trained on personal data except for those clearly set out in the AI Adoption Register.

Where personal data is involved, DDLETB employees that use the AI systems must comply with GDPR and the Data Protection Act 2018 (as amended). DDLETB employees must adhere to DDLETB's Data Protection Policy and Data Retention Schedule.

All Users must adhere to DDLETB's Data Protection Policy.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

17. Incident Report

In addition to Users' responsibilities regarding reporting a suspected data breach, if a User identifies any suspected risks or issues with a particular AI system such as biases, algorithmic errors or security vulnerabilities, s/he must contact his/her Line Manager/ICT Team member immediately so that the risk can be mitigated or the issue resolved as quickly as possible.

18. Other Relevant Policies & Documents

This Policy is to be read in conjunction with the following policies and documents:

- DDLETB's Data Breach Protocol
- DDLETB's Data Processing Policy
- DDLETB's ICT Acceptable Usage Policy
- DDLETB's Code of Conduct for Employees
- DDLETB's Dignity and Respect at Work Charter
- DDLETB's Equality Inclusion Policy

19. Enforcement

Users who are 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 relevant to that user.

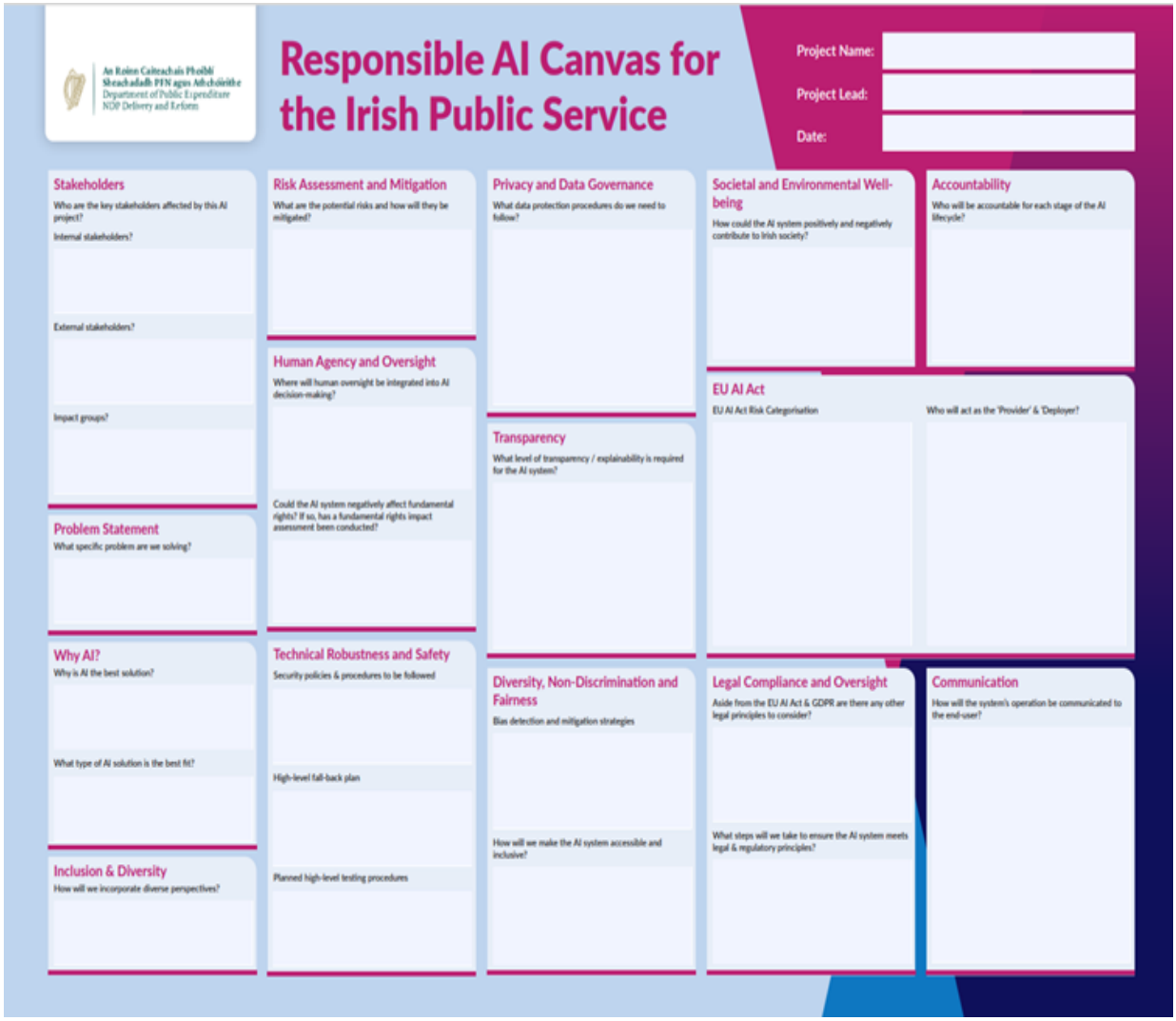
20. Review of this Policy

This Policy has been approved by senior management, who are committed to the ethical, secure, and transparent adoption of AI technologies in DDLETB, together with ensuring alignment with legal obligations under the AI Act and other relevant legislation.

This document will be reviewed at least annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within DDLETB.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

Appendix 1. Responsible AI Canvas for Public Service



Available: Responsible_AI_Canvas.pdf and https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/publications/artificial-intelligence-resources/

Appendix 2. Guidelines for Ethical AI Usage in DDLETB (Do's and Don'ts)

Do's

- ✓ **Ensure Human Oversight**: Always maintain human control and intervention in AI systems to prioritise ethical decision-making.
- ✓ **Verify AI Responses**: AI systems can provide hallucinations which is false information therefore responses from AI systems must be verified by a human to ensure their accuracy.
- ✓ **Conduct Risk Assessments**: Perform thorough risk assessments for high-risk AI systems before approval to determine potential risks.
- ✓ **Promote Transparency**: Clearly state when AI tools are used in work and ensure that AI-generated content is not presented as original work.
- ✓ **Safeguard Data**: Protect personal data and ensure secure data handling in compliance with regulations like GDPR.
- ✓ **Provide AI Training**: Management must provide staff with the necessary knowledge and training to understand and use AI systems responsibly. Staff complete such training where required to do so by management.
- ✓ **Monitor AI Systems**: Continuously monitor AI systems for performance and security risks, and conduct periodic AI audits.
- ✓ **Foster Diversity and Fairness**: Avoid unfair bias in AI systems and ensure that AI-generated content is ethical and non-discriminatory.
- ✓ **Consider Environmental Impact**: Use AI tools responsibly to minimise energy consumption and carbon emissions.

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED

Don'ts

- ☒ **Don't Use Black-box AI**: Do not use AI systems that lack transparency and explainability, as they can affect public trust.
- ☒ **Don't Input Personal Data**: Do not input personal, confidential, or sensitive company information into AI applications.
- ☒ **Don't Encourage Unethical Use**: Do not use AI applications to generate content for bullying, harassment, or any explicit or offensive purposes.
- ☒ **Don't Use for Non-Work purposes**: Do not use AI tools for personal or non-work-related tasks on ETB systems or accounts.
- ☒ **Don't Use Unauthorised AI**: Do not use AI systems that are prohibited under the EU AI Act or those that are listed in the ETB's AI Adoption Register

ONLINE VERSION IS CONTROLLED. DOWNLOADED AND/OR HARD COPY IS UNCONTROLLED