MUUVMENT

A PRACTICAL AI GOVERNANCE TOOLKIT

For responsible, sustainability-focused AI deployment and use

Prepared by **Christa Schweizer**, MBA, MA (Law) in collaboration with
Zabi Yaqeen, General Counsel and Co-Founder, Muuvment Ltd.

v. 1.0. January, 2026

MUUVMENT

This AI Governance Toolkit is designed for small and medium-sized enterprises (SMEs) and is broadly relevant to different sectors and jurisdictions. It is particularly relevant for sustainability professionals as AI is increasingly used in climate strategy, ESG reporting, supply chains and workforce decision-making. It positions AI governance as an extension of an organisation's sustainability framework to enable sustainability teams to identify AI-related risks, influence governance controls, and ensure AI deployment supports credible environmental, social and governance outcomes.

This Toolkit is informed by recognised international AI governance standards and guidance, providing a practical and credible foundation for responsible, sustainability-aligned AI deployment, including:

- the EU AI Act,
- OECD AI Principles,
- NIST AI Risk Management Framework
- ISO/IEC 42001 (AI Management Systems),
- Corporate Sustainability Reporting Directive

and other authoritative frameworks. The toolkit supports SMEs in building trust, ensuring accountable AI use, integrating sustainability considerations, and advancing innovation through ethical and transparent AI use.

> **Important Note:** This AI governance toolkit and the template documents (including the AI Use Policy) are provided for general guidance only. They do not constitute legal advice. Organisations should adapt the materials to their specific context and seek appropriate legal or professional advice to ensure compliance with applicable laws and regulations.

Table of Contents

1. Key Terms

Below are key terms that help build a practical understanding of AI and support the development of a prudent and proportionate governance framework. Some terms are used throughout this toolkit, while others are included to give additional context around AI systems and their responsible use.

Artificial Intelligence (AI) or AI System – a machine-based system that uses data and algorithms to perform tasks that would otherwise require human judgement, such as generating content, making predictions, ranking options or supporting decisions. AI systems may operate with varying levels of autonomy and may change their behaviour over time as they learn from new data or inputs.

AI Use Policy – an internal policy that sets out how AI tools may and may not be used within an organisation, including permitted use cases, data handling expectations, oversight requirements and alignment with sustainability and ethical standards.

AI Impact Assessment – a structured process used to identify and evaluate the potential broader effects of an organisation's use of an AI system on people, society, the economy, the environment and the organisation itself. This includes considering impacts on fairness, inclusion, transparency, workforce practices, environmental footprint and stakeholder trust, and identifying measures to prevent or mitigate negative outcomes before and during use.

AI Risk Assessment – a systematic evaluation of the risks associated with the design, deployment and use of an AI system. This includes legal, ethical, operational, reputational and sustainability-related risks, such as unintended bias, inaccurate outputs, over-reliance on automation or misalignment with sustainability commitments, and the controls needed to manage those risks responsibly.

AI Risk Register – a structured record used to identify, assess, and manage risks arising from an organisation's use of AI systems. The AI Risk Register captures key risk areas such as legal, ethical, operational, data protection, security, reputational, and sustainability-related risks associated with AI use, together with corresponding mitigation measures, ownership, and review status.

Bias – a systematic tendency for an AI system to produce outcomes that unfairly advantage or disadvantage certain individuals, groups or perspectives. Bias can arise from data, model design, assumptions or how outputs are used, and may result in discriminatory, misleading or unbalanced outcomes that undermine social equity and organisational credibility.

Data Protection Impact Assessment (DPIA) – a structured assessment used to identify and manage risks to individuals' privacy and rights when personal data is processed, including through AI systems.

Explainability – the extent to which an AI system's outputs and decision logic can be understood and explained to relevant stakeholders, thereby supporting transparency, trust and regulatory compliance, particularly where AI affects people, reporting or material decisions.

Hallucinations – outputs generated by an AI system that appear plausible but are factually incorrect, misleading or unsupported by reliable data. In sustainability and ESG contexts, hallucinations can create risks where AI is used for reporting, analysis or decision support, potentially leading to inaccurate disclosures or poor decisions.

Human Oversight – processes and controls that ensure humans remain responsible for reviewing, validating and, where necessary, overriding AI outputs. Human oversight is critical to prevent inappropriate reliance on AI and to support accountable decision-making.

Large Language Model (LLM) - a type of AI model trained on large volumes of text data to understand and generate human-like language. LLMs are commonly used in chatbots, content generation and research support tools such as ChatGPT and Copilot, but require careful governance due to risks relating to accuracy, bias, confidentiality and appropriate use.

Lifecycle Management – the approach taken to govern an AI system from initial procurement or development through deployment, ongoing monitoring, updates and eventual retirement, ensuring risks and impacts are managed over time.

Model Drift – changes in an AI system's performance or behaviour over time as data, inputs or operating conditions change, potentially leading to reduced accuracy or unintended outcomes if not monitored.

Prompt Engineering – the practice of designing and refining instructions given to an AI system to influence the quality, relevance and reliability of its outputs. Effective prompt design can improve usefulness and reduce risk, but does not replace the need for human judgement, verification and governance controls.

Small Language Model (SLM) – a more compact language model designed to perform specific tasks using less data and computing power than large language models. SLMs may offer advantages for SMEs seeking greater control, lower environmental impact and reduced risk exposure when deploying AI for defined use cases.

Transparency – making clear when natural persons are interacting with an AI System and providing enough information for them to understand the system's purpose and role. Individuals should be informed that AI is being used unless this is obvious in the context. Transparency supports informed use, appropriate reliance on AI outputs, and effective Human Oversight.

2. Governance Framework

2.1 Core Principles:

An organisation should be guided by the following core principles when assessing implementation of an AI system:

- **Lawfulness**: Ensure AI systems and their use consistently comply with applicable laws and regulations in all jurisdictions of operation.

- **Transparency**: Embed clarity and openness into AI use by maintaining understandable documentation of system purpose, data sources, limitations and changes over time, and by being open with users and affected stakeholders where AI influences outcomes.

- **Reliability**: Ensure AI systems deliver consistent, accurate and dependable outputs, supported by ongoing testing and monitoring throughout their use.

- **Accountability**: Assign internal responsibility for AI-related outcomes and establish clear oversight mechanisms.

- **Fairness and Non-Discrimination**: Identify and mitigate bias in data and use to prevent discrimination and ensure fairness in outcomes.

- **Privacy and Data Protection:** Adhere to data protection standards such as GDPR and equivalent frameworks.

- **Environmental Responsibility**: Ensure AI applications minimise environmental harm, such as energy/water usage and hardware waste).

- **Social**: Avoid causing social harm, including unfair treatment, exclusion or adverse impacts on individuals or communities, and support equitable and inclusive outcomes.

- **Human Oversight**: Ensure meaningful human control over AI systems, particularly those considered high-risk.

- **Safety and Robustness**: Adopt secure and reliable AI practices and apply safeguards to prevent misuse and harmful outcomes.

2.2. Example Governance Structure:

Clearly identify who is responsible for the assessment, implementation, and use of AI systems within the organisation. A proposed governance structure is below but can be adapted to reflect an organisation's resource realities.

Role	Responsibility	Rationale	Reasonable Alternatives
Board of Directors	Highest level of accountability on AI governance oversight across the organisation. The Board may delegate to an AI governance committee or to an existing governance or risk committee.	The Board has ultimate responsibility for strategy, risk management and legal compliance. AI can create material legal, operational and reputational risks, so board-level oversight ensures accountability, appropriate resourcing and alignment with the organisation's objectives and values.	If there is no formal Board, assign accountability to the owner, managing director or senior leadership team. Oversight can sit with an existing risk, audit or ESG committee, or a named executive sponsor reporting to leadership.

Role	Responsibility	Rationale	Reasonable Alternatives
AI Governance Lead	Coordinates AI governance activities and ensures compliance, including policies, procedures, AI risk management and board/employee training.	A single accountable owner prevents AI governance being fragmented across teams. This role coordinates policies, risk management, approvals, training and reporting, and provides a clear escalation point for higher-risk AI use.	If a separate AI Governance Lead role is not feasible, allocate to an existing role such as COO, Head of Operations, Legal, Risk, IT or Sustainability. In smaller SMEs, this may be a shared role or small working group with a named lead. External support can be used with internal ownership retained.
Data Protection Officer (**DPO**)	Oversees data privacy and protection compliance regarding use of personal data in AI tools and projects.	Many AI systems process personal data, directly or indirectly. DPO oversight ensures compliance with data protection law, DPIAs, vendor controls and incident management to reduce regulatory and reputational risk.	Where no formal DPO exists, assign responsibility to a Privacy, Compliance, Legal, HR or Information Security lead, or use an external DPO or advisor with clear internal accountability.
AI Development Team	Implements responsible AI design and testing.	Teams building or configuring AI are best placed to embed responsible design, testing, documentation and monitoring into the system itself, rather than relying solely on policy controls.	If AI is not developed in-house, assign responsibility to IT, product or the business owner of the AI tool. For third-party tools, rely on vendor assurances, internal testing and contractual safeguards.
Ethics Officer	Reviews ethical implications of AI projects.	AI can raise ethical and social issues beyond legal compliance, including fairness, inclusion, trust and impacts on individuals or groups. An ethics review function helps the organisation align AI use with organisational values and sustainability commitments.	For most SMEs, this can be a cross-functional review involving a sustainability, governance, or HR lead, or an external advisor for higher-risk use cases.

3.Internal AI Assessments

3.1 AI Risk Assessment:

Complete a risk assessment for each AI system using a standardized checklist before deployment and at regular intervals thereafter for delayed or latent risks as follows:

i. **List the AI system(s) under review**. Clearly describe each system's intended purpose and expected benefits.

ii. **Identify and assess risks.** Consider risks relating to the AI system's design, data inputs, decision logic, deployment context and any third-party components. This should include technical, legal, ethical, operational and societal considerations.

iii. **Rate each risk as low, medium or high**. For medium- or high-rated risks, define and implement proportionate mitigation measures such as data-quality controls, human oversight requirements, bias testing, system logging, transparency measures and cyber security safeguards.

iv. **Document all assessment findings, decisions and mitigation measures**. Review and update the assessment as part of the organisation's regular governance cycle or when the AI system undergoes significant changes.

v. **Maintain a risk register**. Record identified risks, risk ratings and tolerance level, mitigation strategies, responsible owners, and review dates. The register should cover areas such as bias and fairness concerns, data-privacy risks, cybersecurity vulnerabilities and operational disruptions.

A template AI risk assessment checklist is included at ***Schedule 'A'****, and a template AI risk-register template is included at* ***Schedule 'B'****. Each template includes an example entry for reference.*

3.2 Conduct an AI Impact Assessment:

Develop a framework for assessing the social, economic, and operational impacts of AI systems prior to implementation.

i. **List the AI system(s) under review**. Clearly set out the intended purpose, expected benefits, and whether the AI system is internally developed or provided by a third party.

ii. **Identify all relevant stakeholder groups**. Consider the groups that could be affected by the AI system, including:

- *Employees* – consider effects on job roles, required skills, workload, safety, data privacy, and HR decisions.

- *Customers* – consider effects on service quality or delivery, decision transparency, data privacy expectations and fairness.

- *Suppliers and partners* – consider effects on contractual obligations, data sharing and supply chain continuity.

- *Regulators (if applicable)* – consider any specific regulatory responsibilities or reporting requirements.

- *Wider community and Environment* – consider effects on local employment, human rights, vulnerable groups (e.g. children, the elderly, disabled persons), public trust and perception, and environmental footprint.

iii. **Evaluate both short (0-12 months) and longer-term (1-3 years) effects of the AI system.** For each group, pay particular attention to:

- *Employment and skills impact* – whether the AI system displaces, augments or creates jobs. Identify training, reskilling or job redesign measures may be required.

- *Service-delivery impact* – how the AI system changes accessibility, speed, reliability and fairness of the offered product or service.

- *Operational impact* – determine any dependencies, integration complexities, staff oversight needs, and any impact on business continuity.

- *Economic impact* – cost-benefit analysis, potential market advantages, and risks of over-reliance on automated processes.

- *Societal impacts* – consider potential discrimination, transparency, user trust and broader societal implications of adopting the AI system.

iv. **Assign a risk level as low, medium or high for each impact area**. The rating should reflect the potential seriousness of the effect on stakeholders, operations and/or the environment.

- *Low risk*: minor or negligible impact (no immediate mitigation needed).

- *Medium-risk*: noticeable impact that could affect trust, compliance or performance (mitigation actions should be defined).

- *High-risk*: significant impact that may lead to legal, regulatory, reputation, and/or safety consequences (urgent mitigation required).

- *Prohibited*: AI system and/or use case that is legally restricted or has been deemed by the organisation to present unacceptable risk and must not be used.

v. **Determine mitigation measures for medium- and high-risk impact areas**. Specify the following:

- Controls to reduce or manage the impact.
- Monitoring and reporting mechanisms, including human oversight.
- Training or communication needs.
- Decision points for go/no-go deployment.

*A template AI impact assessment template can be found at **Schedule 'C'** with an example entry for reference.*

3.3 Ethics Assessment:

Carry out an assessment of how the organisation's use of an AI system impacts fair outcomes and potential bias.

i. **Conduct a data audit (pre-deployment)** to examine the data that will be used in the AI system and evaluate outputs for potential bias or unfair outcomes. Consider whether predictions or recommendations could disproportionately affect specific groups.

ii. **Define fairness metrics** by establishing specific metrics relevant to the organisation's context, such as demographic parity and equal opportunity, to monitor bias systematically.

iii. **Engage relevant internal stakeholders** such as HR, Legal, Risk, and Operations to flag potential fairness issues.

iv. **Carry out a regulatory check** to identify any jurisdiction-specific fairness, discrimination, or AI regulations that may apply.

v. **Scenario Testing**: Run simulations or pilot tests on sample data to identify unexpected biases before full deployment.

vi. **Require prior approval** from the AI Governance Lead, Ethics Advisor, or equivalent before deployment to ensure accountability.

A template to document the AI ethics assessment can be found at **Schedule 'D'** with an example entry for reference.

3.4 Data-Protection Impact Assessment:

Many organisations will already be assessing the impact of their systems, processes and decisions on personal data through established Data Protection Impact Assessment (**DPIA**) documentation. However, where an AI system is involved, a DPIA should go further than a traditional privacy assessment. In addition to the organisation's existing DPIA framework and internal risk processes, the organisation should explicitly consider the following steps:

i. **Determine whether a DPIA is required**. Identifying if the AI system processes personal data in a way that may create high-risk, including automated decision making, behavioural monitoring or the use of special category data.

ii. **Clearly describe the AI system and purpose**. Set out what the AI system does, how it will be used, the data it relies on and why the organisation needs it.

iii. **Map and assess the data**. Identify the personal data involved, where it comes from, how it is stored and retained and whether it is necessary and reliable.

iv. **Identify privacy risks to individuals**. This could include confidentiality breaches, unfair or discriminatory outcomes, inaccurate inferences or unauthorised access.

v. **Check compliance with applicable privacy laws**. Ensure alignment with relevant frameworks such as UK and EU GDPR, PIPEDA, US state laws, including lawful basis, Transparency and individual rights.

vi. **Review safeguards**. Assess whether technical and organisational controls are sufficient, including human review and monitoring, data minimisation, access controls, and encryption.

vii. **Assess AI-specific considerations**. Confirm that the system offers appropriate levels of Explainability, transparency, fairness checks, monitoring and the ability to intervene or override automated decisions.

viii. **Review third party arrangements**. Check contractual protections, server locations, data-sharing terms and the vendor's data protection standards.

ix. **Consult internal stakeholders**. Validate assumptions and identify any operational issues.

x. **Document decisions and residual risks**. Record the risks identified, the controls adopted and the rationale for deployment. Obtain senior approval where high residual risks remain.

xi. **Update the DPIA as AI-system evolves**. This could be as a result of system updates, new data sources, changes in use or new regulatory requirements.

xii. **Retain the DPIA for governance purposes**. Ensure it is available for internal review or regulatory requests as applicable.

Schedule 'E' sets out a template DPIA (with an example entry for reference) that can be used to assess the privacy risks associated with an AI system and the controls required to manage them.

3.5 Industry-Specific Assessments:

Organisations should be aware that certain industries have additional assessment requirements or good-practice expectations when using AI. Organisations can refer to **Schedule 'F'** for a non-exhaustive list of industry-specific considerations to ensure that their planned use of AI meets the standards and regulatory obligations of their sector.

4. AI Policy and Compliance

4.1 AI Use Policy:

Develop and maintain an internal AI Use Policy that sets clear expectations for responsible, transparent and accountable AI use across the organisation. The policy should be informed by the outcomes of its internal assessments (e.g. AI risk, impact, ethics, and data protection), industry and jurisdiction specific legal considerations, as well as the organisation's overall AI strategy, values, culture, and risk tolerance.

At a minimum, the AI Use Policy should cover the following areas:

i. **Purpose & Scope**: explain why the policy exists, what it covers and who it applies to (e.g. all directors, employees, contractors, suppliers etc.).

ii. **Core Ethical Principles**: state the organisation's guiding values, such as fairness, transparency, accountability, data privacy, and respect for human rights.

iii. **Acceptable AI Applications**: clearly define approved and prohibited uses of AI within the organisation's business context (e.g., customer service chatbots, fraud detection, HR screening).

iv. **Responsible Use Parameters**: set parameters around approved AI use cases and levels of use to ensure AI systems are used only for clearly defined and documented purposes that deliver genuine value. Avoid excessive or low-value use, taking into account potential social impacts such as fairness and human agency, as well as the environmental footprint of AI systems, including energy use and resource intensity.

v. **Human Oversight and Accountability**: identify roles and responsibilities, such as who approves AI tools and tracking such approvals, who monitors performance and end-of-life processes, and how human review is maintained for critical decision-making.

vi. **Data Protection**: include provisions that clearly protect personal data (particularly special categories of personal data e.g. racial or ethnic origins and biometric data) and/or ensure the policy reinforces obligations under the organisation's data protection policy.

vii. **Policy Review and Updates**: outline how the policy will be reviewed and updated to reflect emerging regulations, best practices, and lessons learned from AI use in your organisation.

viii. **Training**: provide clear and understandable training on responsible AI use to all whom the AI use policy applies at least annually, document each training session, and include a proportionate mechanism to confirm understanding, such as a short knowledge check or attestation.

ix. **Review**: ensure there are periodic review mechanisms to update the policy as needed to comply with regulatory changes and incorporate best practices.

x. **Employee sign-off or confirmation of compliance**: require documented employee acknowledgement of the AI Use Policy and establish proportionate monitoring and enforcement mechanisms.

A template AI Use Policy can be found at ***Schedule 'G'*** to this toolkit.

4.2 Compliance:

The following set the baseline for complying with the legal, regulatory and internal/external governance requirements for AI deployment.

i. Align the AI Use Policy with the EU AI Act's risk-based approach by classifying AI tools under prohibited, high-risk, limited-risk, minimal-risk systems.

ii. Consider jurisdiction-specific compliance obligations, regulatory requirements and governance expectations applicable to the organisation when deploying an AI system and continue to monitor these throughout its use. ***Schedule 'H'*** sets out a non-exhaustive list of jurisdictional legal, regulatory and governance frameworks that organisations operating in those locations should review prior to deployment and on an ongoing basis.

iii. Review the organisation's existing internal policy framework and cross-reference the AI Use Policy with all relevant policies (e.g. cyber-security and risk-management) to ensure alignment, avoid contradictions, and address any overlapping responsibilities.

iv. Require that every employee who utilizes an AI system in the course of their employment acknowledges that they have read, understood, and will comply with the AI Use Policy.

5. On-Going Monitoring

5.1 Key Performance Indicator (**KPI**) Tracking

The organisation should track relevant performance metrics to ensure continued accuracy, fairness, safety and reliability following deployment of the AI system. KPIs may include:

- Accuracy, precision and error rates
- Fairness metrics (e.g., demographic parity ratios, false-positive disparities)
- Reliability measures (e.g., uptime, latency, consistency)
- Explainability outputs (if applicable)
- User feedback, error reports and complaint patterns
- Changes in input data quality, relevance, or patterns over time

KPIs should be reviewed at scheduled intervals and benchmarked against baseline performance established during testing.

5.2 Post-Deployment Monitoring Requirements

Post-deployment monitoring should be in place to detect unintended consequences, Model Drift, misuse or emerging risks. Monitoring should ensure that:

- Outputs remain consistent with expected behaviour
- The AI System does not produce discriminatory, unsafe or unreliable outcomes
- Model performance has not deteriorated due to new data patterns, environmental changes or external factors
- Any changes made by third-party suppliers (e.g., model updates) are logged and reviewed
- Human Oversight remains active, meaningful and documented

Monitoring frequency should be risk-based:

Risk level	**Visual indicator**	**Review frequency**
High/business critical	🟥 (Red)	Continuous or weekly
Moderate	🟨 (Amber)	Monthly or quarterly
Minimal	🟦 (Blue)	Periodic spot-checks

5.3 Automated Alerts and Anomaly Detection

Where possible, the organisation should incorporate automated triggers to flag:

- Sudden drops in accuracy or reliability
- Unexpected output patterns
- Data-drift signals
- Security anomalies (e.g., unusual system access)
- Sustained fairness deviations
- Failed integrations or API errors

Alerts should be sent to designated owners (e.g., AI Governance Lead, IT Lead or Risk Officer) with clear escalation mechanisms.

5.4 Mechanisms for Override, Audit and Decommissioning:

The organisation should maintain controls that allow for:

- Override or human intervention when outputs appear incorrect or harmful
- Audit trails capturing key inputs, decisions, parameters, updates and exceptions
- Temporary suspension if the system exhibits unsafe or non-compliant behaviour
- Full decommissioning if risks cannot be mitigated or if the system is no longer appropriate or lawful

Decommissioning procedures should include:

- Removal of system access
- Secure archiving or deletion of associated datasets
- Communication to affected stakeholders
- Updating relevant documentation and the AI Risk Register

6. Internal and External Communication

The organisation should develop clear internal and external communication around AI use to build trust, reduce confusion and ensure compliance with legal requirements and regulatory requirements, such as data protection laws, consumer protection laws and EU AI Act Transparency rules.

6.1 Privacy Statement and Notice Updates

If an AI system processes personal data or makes decisions affecting individuals, the organisation should consider whether its privacy notices need to be updated to reflect:

- The fact that AI is used
- The purpose of the AI system
- The categories of data used
- Whether any automated decision-making is involved
- The lawful basis for processing (e.g., legitimate interests, consent)

- The individual's rights (e.g. right to explanation where applicable)
- Contact details for further queries or complaints

Updates should be communicated through existing channels (e.g., website, privacy notices, onboarding materials, contract updates).

6.2 Transparency on AI Use

The organisation should provide clear information to relevant stakeholders, including employees, customers, suppliers, regulators and the wider community when interacting with or being affected by AI systems.

i. Transparency measures may include:

- Labelling AI-generated or AI-supported content
- Informing employees when internal tools (e.g., HR, workflow automation) rely on AI
- Brief, easy-to-understand descriptions of AI capabilities
- Disclosure of limitations (e.g., potential for errors, reliance on training data)
- Information on human oversight mechanisms
- A point of contact for queries or concerns

ii. Transparency should be proportionate to the AI System's impact and context.

7. Board & Employee AI Training

Continuous learning is core to responsible AI adoption. Training should reflect the organisation's scale, risk profile and governance maturity.

7.1 Regular Training for Directors and Staff

All board directors, senior leaders, employees and contractors using AI systems as part of their work for the organisation should receive periodic training covering:

i. Basic AI concepts and terminology
ii. Organisational AI Use Policy
iii. Use cases, including parameters that reflect environmental considerations
iv. Ethical principles such as fairness, Transparency, accountability and safety
v. Data protection requirements (e.g., data minimisation, lawful bases)
vi. Recognising and escalating potential AI-related risks
vii. Human Oversight responsibilities
viii. AI-specific cybersecurity basics (e.g., prompt injection, model misuse)

Training should be refreshed at least annually or when new AI Systems or tools are introduced.

7.2 Awareness Materials and Practical Guidance

Develop practical materials that support day-to-day responsible AI use, such as:

i. One-page guides on safe and compliant AI use
ii. Do-and-don't sheets for using AI tools, particularly those classified as generative AI
iii. Short videos or FAQs
iv. Checklists for staff evaluating AI outputs
v. Practical examples of good oversight and error detection

These materials should be accessible, jargon-free and tailored to the organisation's business.

8. AI Governance Checklist

□ Identify and assign accountability for AI use in the organisation

□ Define organisational values and principles for AI deployment and use

□ Conduct internal assessments of AI risk, impact, ethics, and data protection proportionate to nature and use of AI System

□ Consider AI-related laws, regulations and standards applicable to the organisation's industry and jurisdiction of operation

□ Adopt and maintain an AI Use Policy that is clear, practical to implement ,and appropriate for the organisation's size, resources and risk profile

□ Implement an ongoing AI monitoring process

□ Ensure internal and external communication on AI deployment and use are clear, accurate and appropriate for relevant stakeholders

□ Provide periodic, role-appropriate training for board members, employees, and contractors on responsible AI use and governance expectations

□ Develop AI awareness materials and guidance notes to support staff in using AI Systems responsibly and in line with the AI Use Policy

Schedule ‘A’
Template AI Risk Assessment

How to Use This Template

1. Identify the AI system and its intended purpose & benefits.
2. Select the relevant risk area (<u>see common risk areas</u>).
3. Describe the risk clearly, stating what could go wrong and who or what may be affected.
4. Rate the risk level (Low / Medium / High), based on likelihood and impact.
5. Document existing and planned mitigation measures that reduce or manage the risk.
6. Assign an owner responsible for monitoring the risk and set a review date.

Common Risk Areas to Consider

- *Technical Performance*: inaccuracies, instability, dependency on vendor systems.
- *Data Quality and Data Protection*: poor data integrity, inappropriate data use, privacy risks.
- *Fairness and Bias*: unfair outcomes affecting groups or individuals.
- *Ethical or Societal Risk*: risks to autonomy, transparency, trust or public welfare.
- *Sustainability*: excessive energy use, negative impacts on sustainability commitments.
- *Operational Risk*: overreliance on outputs, lack of human review, workflow disruption.
- *Legal/Regulatory*: sector rules, consumer protection, employment law
- *Third-Party / Vendor Risk*: unclear assurance from providers, data-sharing risks.
- *Cybersecurity*: vulnerabilities introduced through AI tools or integrations.

Template AI Risk Assessment Table:

AI System	Purpose & Expected Benefits	Risk Area	Description of Risk	Risk Level (L/M/H)	Mitigation Measures (Existing or Planned)	Owner	Review Date
E.g. EcoPredict	*Cloud-based AI forecasting tool to optimize stock levels and logistic*	*Sustainability*	*The AI forecasting tool requires regular cloud-based model retraining. Increased compute demand may drive unnecessary energy use and conflict with the organisation’s sustainability commitments, including carbon-reduction targets.*	*Medium*	*Use energy-efficient model settings, limit retraining frequency to what is operationally necessary, select cloud providers with renewable-energy commitments, track estimated emissions impact.*	*Head of Sustainability*	*June 2026*[1]

[1] The review date can once a quarter, every 6-months or at such intervals as the organisation deems appropriate, provided the review is carried out within a year.

Schedule ‘B’

Template AI Risk Register

AI System	System Type	AI Use Case(s)	Risk Description	Risk Rating	Likelihood[2]	Risk Tolerance Level	Mitigation / Action Required	Owner	Review Date
E.g. Microsoft Copilot	*Generative AI Assistant*	• *Document drafting and editing* • *Productivity and workflow support* • *Search and knowledge retrieval* • *Data analyses and reporting* • *Internal communications support*	*Staff may input confidential or sensitive information that is not appropriate for Copilot’s context window, creating risks of data leakage, misinterpretation of content, or ESG misalignment if outputs are used without adequate review.*	*Moderate*	*Possible*	*Within approved limits*	*Provide mandatory training on approved use cases and prohibited inputs; enable appropriate Microsoft 365 data-access controls; require human review of all outputs prior to external use; monitor usage through admin dashboards.*	*IT Manager*	*1 May 2025*[3]

[2] Likelihood categories:
Rare - could happen only in exceptional circumstances
Unlikely - No expected to occur but still possible
Possible - may occur at some point, and there is reasonable chance of it happening.
Likely - Expected to occur at some point; has happened before or is happening elsewhere in the organisation.
Almost certain - high probability of occurring; occurs frequently or is already happening.

[3] The review date can once a quarter, every 6-months or at such intervals as the organisation deems appropriate, provided the review is carried out within a year.

Schedule 'C'

Template AI Impact Assessment

How to Use This Template

1. Describe the AI system, its purpose, expected benefits and impact area.
2. Identify affected stakeholders including employees, customers, suppliers, regulators, the community and the environment.
3. Consider short-term (0–12 months) and long-term (1–3 years) impacts.
4. Assign a risk level (Low / Medium / High).
5. Determine mitigation measures such as controls, oversight, reporting, training and decision criteria.

Suggested Impact Categories

- Employment and Skills
- Service Delivery
- Operational Changes
- Economic and Financial Impact
- Fairness and Societal Impact
- Environmental / Sustainability Impact
- Data and Privacy Expectations
- Community and Reputational Impact

Template AI Impact Assessment Table:

AI System	Purpose & Expected Benefits	Impact Area	Stakeholder Group(s) Affected	Short-Term Impact (0–12 months)	Long-Term Impact (1–3 years)	Risk Level (L/M/H)	Mitigation Measures	Owner	Review Date
E.g. DeliverAssist AI	*Automated assistant generating real-time delivery updates and ETAs to speed responses, improve customer communication and ease customer-service workload.*	*Delivery Service*	*Customers*	*Faster response times but risk of incorrect automated responses.*	*Possible reduced trust if inaccuracies persist.*	*Medium*	*Human-in-the-loop review, monthly accuracy checks, staff escalation training, update customer communication.*	*Head of Customer Service*	*June 2026*

Schedule ‘D’

Template AI Ethics Assessment

How to Use This Template

1. Describe the AI system, its purpose and expected benefits.
2. Identify affected stakeholders such as employees, customers, and community members
3. Document ethical concerns arising from outcome of core checks (e.g. data audit, fairness metrics)
4. Assign an ethics risk level (Low / Medium / High).
5. Record mitigation measures including controls, oversight, and training.
6. Determine if any approvals are required and assign a review date.

Suggested Ethical Areas to Consider

- Fairness and Bias
- Transparency and Explainability
- Autonomy and Human Oversight
- Accountability and Governance
- Human Rights and Harm Prevention
- Cultural and Social Impact

Template Ethics Assessment Table:

AI System	Purpose & Expected Benefits	Ethical Area	Description of Ethical Concern	Affected Stakeholder(s)	Ethics Risk Level (L/M/H)	Mitigation Measures	Owner	Approval Required (Y/N)	Review Date
E.g. Ada	*Customer-service chatbot that provides automated responses to common customer queries.*	*Fairness and Bias*	*Data audit identified that historical customer-service records under-represent older customers, leading to the risk that automated responses may not address their needs effectively. Scenario testing indicated occasionally*	*Customers, particularly older adults and those less familiar with technology.*	*Medium*	*Expand training data to include more representative examples, monitor fairness metrics monthly, include a “request human support” option in all*	*Head of Customer Experience*	*Yes*	*September 2026*

			less accurate or less helpful responses for this demographic.			*interactions, and conduct quarterly scenario tests.*			

Schedule 'E'

Template DPIA

1. Set out AI System Details

AI System	System Type	Vendor / Developer	Business Owner	Date Initiated	Version Number	Review Cycle	Completed By	Approval Required (Y/N)
E.g. Copilot	*Large Language Model (LLM) assistant integrated within Microsoft 365*	*Microsoft*	*Head of IT / Digital Transformation Lead*	*1 January 2026*	*v1.0 (initial deployment)*	*Annual, or earlier if significant updates occur*	*Data Protection Officer*	*Yes*

2. DPIA Screening – Is a DPIA Required?

Screening Question	Yes/No	Notes
(a) Does the AI system process personal data?		
(b) Does it involve automated decision-making that could affect individuals?		
(c) Does it monitor behaviour, location or performance?		
(d) Does it involve special category data or data on vulnerable individuals?		
(e) Could the system create high-risk to individuals' rights or freedoms?		

Outcome (select one): DPIA Required □ Not Required □

If not required, provide rationale: ____

3. Template DPIA Findings:

Assessment Area	Summary of Findings	Identified Risks to Individuals	Mitigation Measures (Existing or Planned)	Residual Risk (L/M/H)	Owner	Review / Update Required (Y/N)
Data Mapping & Necessity	*E.g. Copilot processes data already held in Microsoft 365, including emails, documents, Teams messages and calendar entries. No new data collection, but broad access to employee content.*	*Risk of excessive data exposure if employees store unnecessary personal information in documents or emails. Risk of Copilot surfacing information to the wrong user if permissions are misconfigured.*	*Enforce organisational data-classification policy, reduce unnecessary personal data in M365 content, review access permissions.*	*Medium*	*IT Security Lead*	*Yes*
Privacy Risks to Individuals						
Compliance with Applicable Laws						
Safeguards (Technical & Organisational)						
AI-Specific Considerations						
Third Party / Vendor Risks						

Stakeholder Consultation						
Final Deployment Decision						

Schedule 'F'

Industry-Specific Considerations & Assessments for AI Deployment

Industry	Key Assessments and Considerations
Financial Services	• Algorithmic decision-making review for credit, fraud, AML and onboarding tools. • Model Risk Management (MRM) expectations • Fair lending / anti-discrimination checks for consumer-facing AI tools. • Data quality and Explainability review for high-stakes financial decisions.
Healthcare, Life Sciences and Social Care	• Clinical safety assessments • Regulatory review if the AI tool meets the definition of a medical device under applicable regimes (e.g. UK MHRA, EU MDR). • Patient confidentiality assessments, including enhanced data-protection review where health data is processed. • Bias and safety testing for diagnostic, triage or decision-support systems.
Human Resources and Recruitment	• Bias and fairness audits for hiring, performance evaluation, promotions and automated screening. • Compliance checks with employment and equal opportunities laws (e.g., UK Equality Act 2010). • Transparency assessments where automated decision making is used in HR processes.
Retail, E-commerce and Consumer Services	• Consumer protection and fairness checks for pricing algorithms and personalized recommendations. • Review of marketing and profiling practices against privacy and consumer protection regulations. • Assessment of automated customer-service tools for accuracy, transparency and escalation pathways.
Energy, Utilities and Infrastructure	• Safety and reliability assessments for AI used in grid management, predictive maintenance or operational controls. • Cyber-physical risk assessment where AI interacts with critical infrastructure. • Environmental or sustainability-related assessments where AI influences emissions reporting or environmental claims.
Education and Child-Focused Services	• Safeguarding assessments where data relates to children or vulnerable groups. • Fairness and transparency checks for AI used in grading, learning analytics or behavioural monitoring. • Data-protection review focusing on minimum necessary processing.
Professional Services (Legal, Accounting, Consulting)	• Confidentiality and privilege review for tools processing client information. • Accuracy and reliability checks for AI used in drafting, analysis or research. • Vendor transparency and auditability for third-party SaaS tools.
Public Sector and Non-Profits	• Accountability and proportionality assessments for AI affecting public decisions. • Transparency and Explainability review aligned with public law and administrative fairness principles. • Additional bias and procedural fairness checks for systems impacting services or benefits.

Schedule 'G'
Template AI Use Policy

Effective Date: [●]
Approved By: [*Board / Managing Director / Senior Management*]
Policy Owner: [*Role title, e.g. Head of Sustainability, General Counsel, COO*]
Version: [●]
Next Review Date: [●]

1. Purpose and Scope

1.1 Purpose

This AI Use Policy (**Policy**) establishes a clear, practical framework for the responsible, transparent and proportionate use of Artificial Intelligence within [*insert organisation name*] (the **Organisation**). It is designed to ensure that AI use: (i) supports the Organisation's business objectives; (ii) aligns with the Organisation's values, ethical commitments, and sustainability strategy; and (iii) promotes consistent, well-governed AI use in line with recognised legal, regulatory and good-practice expectations.

1.2 Scope

This Policy applies to all AI Systems that are designed, procured, configured, deployed, accessed or used on behalf of the Organisation, whether internally developed or provided by third parties. It applies to all:

i. Board directors and officers;
ii. Employees (permanent, temporary and secondees);
iii. Contractors, consultants and agency workers; and
iv. Third-party service providers and suppliers acting on the organisation's behalf, where they engage in activities involving AI or AI-enabled tools.

1.3 Relationship to Other Policies

This Policy operates alongside, and does not replace, existing organisational policies, including data protection, information security, sustainability, HR, procurement and risk management policies. Where conflicts arise, the stricter requirement applies.

2. Definitions

For the purposes of this Policy:

Artificial Intelligence (AI) means a machine-based system that uses data and algorithms to perform tasks that would otherwise require human judgement, such as generating content, making predictions, ranking options or supporting decisions. AI Systems may operate with varying levels of autonomy and may change their behaviour over time as they learn from new data or inputs.

AI Ethics Officer means the designated person responsible for providing ethical oversight and guidance in relation to the Organisation's use of AI Systems.

AI Governance Lead means the person responsible for coordinating the Organisation's AI governance activities and ensure compliance, including policies, procedures, AI risk management and board/employee/contractor training.

AI Impact Assessment means a structured process used to identify and evaluate the potential broader effects of the Organisation's use of an AI System on people, society, the economy, the environment and the Organisation itself. This includes considering impacts on fairness, inclusion, transparency, workforce practices, environmental footprint and stakeholder trust, and identifying measures to prevent or mitigate negative outcomes before and during use.

AI Risk Assessment means a systematic evaluation of the risks associated with the design, deployment and use of an AI System. This includes legal, ethical, operational, reputational and sustainability-related risks, such as unintended Bias, inaccurate outputs, over-reliance on automation or misalignment with sustainability commitments, and the controls needed to manage those risks responsibly.

AI Risk Register means a documented record of identified risks associated with the Organisation's use of AI Systems, including legal, ethical, operational, and sustainability considerations, and the measures in place to manage those risks. The AI Risk Register is used to support informed decision-making and ongoing oversight of AI use and is maintained in line with this Policy.

AI System means any software, tool, model, application, or service that is designed to operate with some level of autonomy to generate outputs such as predictions, recommendations, content, or decisions that can influence people or processes. For the purposes of this definition, references to an AI System include any material version updates, configurations or feature changes that may affect its functionality or risk profile.

Bias means a systematic tendency for an AI System to produce outcomes that unfairly advantage or disadvantage certain individuals, groups or perspectives. Bias can arise from data, model design, assumptions or how outputs are used, and may result in discriminatory, misleading or unbalanced outcomes that undermine social equity and organisational credibility.

High-Risk AI Use means AI use that may materially affect individuals' rights, safety, wellbeing, employment, access to services, financial position or environmental outcomes.

Human Oversight means meaningful human involvement with the authority to review, challenge, override or stop AI-supported outputs or decisions.

Personal Data and ***Special Category Data*** have the meanings given under applicable data protection law.

User means any individual who uses an AI System, or relies on its outputs, when performing work for or on behalf of the Organisation, including employees and contractors.

[*Drafting note: adapt or expand these definitions to reflect the Organisation's specific industry and/or regulatory contexts*.]

3. Core AI Principles

All AI use within the Organisation must align with the Organisation’s values, ethical commitments and sustainability objectives, and with the following core principles for responsible AI use. These principles are informed by recognised good practice and international AI governance frameworks, as they evolve over time:

3.1 Purpose-Led and Value-Driven Use

AI Systems must serve a clearly defined, documented and legitimate business purpose that delivers genuine value. AI Systems must not be adopted solely for novelty or convenience.

3.2 Human Agency and Accountability

Humans remain accountable for decisions supported by AI Systems. AI Systems must support, not replace, responsible human judgment, particularly in confidential or sensitive contexts.

3.3 Fairness and Non-Discrimination

AI Systems must be used in ways that seek to prevent unjustified Bias, discrimination or exclusion, with particular care where decisions may affect individuals or groups.

3.4 Transparency and Explainability

Use of AI Systems must be appropriately transparent. Users and affected stakeholders should be able to understand when AI is used, its role in decision-making and its key limitations, to a degree proportionate to risk.

3.5 Privacy and Data Stewardship

Personal Data must be handled lawfully, minimally and securely, with privacy protections embedded by design and by default.

3.6 Safety, Reliability and Security

AI Systems must be reasonably safe, reliable and resilient throughout their lifecycle, with controls proportionate to the level of risk.

3.7 Social and Environmental Responsibility

AI use should consider social and environmental impacts across the AI lifecycle, including fairness, inclusion, accessibility, human agency, energy consumption, compute intensity and associated emissions. Preference should be given, where feasible, to efficient, lower-impact solutions that balance operational benefit with social responsibility and environmental sustainability.

3.8 Continuous Improvement

AI governance practices should evolve based on experience, monitoring outcomes, regulatory developments and emerging best practice.

4. Approved and Prohibited AI Uses

4.1 Approved AI Uses

Only uses of AI Systems that are recorded in ***Schedule I – Approved AI Use Cases*** may be deployed or used for work carried out on behalf of the Organisation. Each approved use case must:

i. have a clearly documented purpose, scope and business owner,
ii. be assessed for legal, ethical, operational and sustainability risks,
iii. comply with this Policy and all related governance, data-protection and information security requirements,
iv. incorporate appropriate Human Oversight,
v. be proportionate to the Organisation's operational need, taking into account compute demand and resource use, and
vi. be recorded in the Organisation's AI Risk Register with their use case, risk rating, risk tolerance level, mitigation requirements, owner, and review date.

4.2 Prohibited AI Applications

i. The Organisation prohibits the use of AI Systems for any purpose listed in ***Schedule II – Prohibited AI Use Cases***, as amended from time to time. Schedule II forms part of this Policy and may be updated independently to reflect changes in law, regulation, organisational risk appetite, sustainability commitments or emerging best practice.

ii. Unless expressly approved in writing by the Policy Owner following a documented assessment, AI use cases falling within Schedule II are not permitted. The Organisation reserves the right to suspend or prohibit any AI use that presents unacceptable legal, ethical, social, environmental or operational risk, whether or not expressly listed in Schedule II.

5. Responsible Use Parameters

5.1 AI Systems must only be used for their approved and documented purposes. Users must:

i. understand the appropriate use and limitations of all AI outputs,
ii. use an AI System only for its intended purpose(s) and not in any way that is inconsistent with its authorised scope, including for personal purposes,
iii. avoid over-reliance on AI-generated content or recommendations,
iv. carefully review outputs for accuracy, relevance and potential Bias before use,
v. remain the ultimate decision-makers and be responsible for applying appropriate judgment when using AI outputs,
vi. escalate concerns or unexpected behaviour promptly to the [*AI Governance Lead/User's reporting manager*].

5.2 Sustainability considerations must form part of AI use decisions, including:

i. selecting model sizes that are less energy-intensive (e.g. smaller or locally run AI systems),
ii. limiting unnecessary, duplicative, or low-value AI use through clear use-case justification,
iii. considering the sustainability credentials of cloud and AI service providers where relevant,

iv. monitoring AI-related energy use and environmental impact on a proportionate, best-efforts basis, relying on available proxy indicators and supplier information, and

v. promoting responsible User behaviour and Human Oversight to avoid excessive or inefficient AI use.

6. Human Oversight and Accountability

6.1 Human Oversight

i. Use of AI Systems are subject to appropriate Human Oversight. AI systems should be used to support, inform, or augment human decision-making and must not be relied upon as the sole basis for decisions that may have legal, ethical, financial, or sustainability impacts.

ii. The level and form of Human Oversight applied to an AI system shall be proportionate to the nature, risk, and potential impact of the AI use case. Higher-Risk AI uses or business-critical AI uses require increased review, scrutiny, and the ability for human intervention, including the ability to question, override, or suspend AI-supported outputs where necessary.

iii. Users remain responsible for exercising professional judgment when using AI Systems and for escalating concerns, errors, or unexpected outcomes in accordance with this Policy.

6.2 Accountability

Responsibility for AI use in the Organisation shall be assigned as follows:

i. *Senior accountability* – overall accountability for the Organisation's use of AI Systems sits with the [*Board of Directors/Senior Leadership*], consistent with the Organisation's responsibility for strategy, risk management and legal compliance. [*The Board/Senior leadership*] may delegate day-to-day oversight to an appropriate governance role but retains ultimate accountability.

ii. *AI Governance Lead* – an AI Governance Lead shall be designated to coordinate the Organisation's AI governance activities. This role is responsible for maintaining this Policy, supporting its implementation, coordinating approvals and reviews of AI use cases, and acting as the primary escalation point for Higher-Risk AI use.

iii. *AI Ethics Officer* – an AI Ethics Officer shall be appointed to work alongside the AI Governance Lead to provide ethical oversight and challenge in relation to AI use, particularly where AI Systems may affect individuals, decision-making, trust, or sustainability commitments.

iv. *AI use case ownership* – each approved AI use case shall have a named business owner responsible for ensuring that the AI System is used in accordance with this Policy, including lawful, ethical and sustainable operation within the defined scope of use.

v. *Users* – all Users are responsible for:

- complying with this Policy and any related procedures,
- completing all required training and related assessments (if any), and
- using them responsibly and only for approved purposes.

Users are not responsible for organisational governance decisions but are expected to raise concerns or potential issues through appropriate escalation channels.

[*Drafting note*: *adapt the accountability structure in line with the reality of the organisation's resource realities*]

6.3 Approvals and Monitoring

All approved AI Systems must be periodically reviewed for performance, risk, Bias, sustainability impacts and ongoing suitability.

6.4 End-of-Life and Exit

AI Systems must have defined review and retirement processes, including data handling and model decommissioning where relevant.

7. Data Protection Requirements

7.1 AI processing must comply with applicable privacy laws and internal data-protection policies. Special-Category Data must only be processed where lawful, necessary and protected by enhanced safeguards.

7.2 Confidential, proprietary or Personal Data must not be input into AI tools unless explicitly approved and adequately protected.

8. Training and Awareness

8.1 All individuals to whom this Policy applies must complete AI use training at least annually.

8.2 Training must be documented and include a proportionate mechanism to confirm understanding, such as an attestation or short knowledge check.

9. Review and Updates

9.1 This Policy will be reviewed at least annually and whenever:

i. New AI regulations or guidance are introduced and/or existing ones materially change,
ii. new High-Risk AI uses are introduced, or
iii. significant issues arise in practice.

9.2 Lessons learned from incidents, audits or User feedback should inform updates.

10. Compliance, Acknowledgement and Enforcement

10.1 Compliance with this Policy is mandatory.

10.2 All relevant individuals must acknowledge this Policy in writing or electronically.

10.3 Breaches may result in removal of AI access, additional training, contractual remedies or disciplinary action, as appropriate.

11. Related Documents

- Data Protection Policy
- Information Security Policy
- Sustainability Policy
- AI Risk Assessment
- AI Impact Assessment
- AI Risk Register

AI Use Policy
Schedule I – Approved AI Use Cases

[*Drafting note:* *the Organisation must document all approved AI use cases for each AI system. AI systems may only be used for the purposes set out in this Schedule.]*

AI System	**Approved Use Case(s)**	**Conditions/Restrictions**	**Review Frequency**

AI Use Policy
Schedule II – Prohibited AI Use Cases

The following AI uses are prohibited:

- Biometric identification of individuals.
- Emotion recognition or behavioural surveillance of individuals.
- Fully automated decision-making with legal, financial, employment or similarly significant effects without meaningful human review.
- AI use that conflicts with the Organisation’s sustainability, human rights or ethical commitments.
- Processing of personal data or special category data without a lawful basis or appropriate safeguards.
- Use of AI systems trained on data where appropriate rights, permissions or licences are not in place.
- Use of AI to mislead, manipulate or deceive.

Schedule 'H'
Jurisdictional Compliance Considerations[4] for AI Deployment & Use

Jurisdiction	**Key Legal & Regulatory Frameworks**	**Governance, Ethics & Additional Considerations**
Canada	- Personal Information Protection and Electronic Documents Act (PIPEDA) - Provincial privacy laws (e.g., Quebec Law 25, Alberta PIPA, BC PIPA) - Artificial Intelligence and Data Act (AIDA) (*proposed*) - Competition Act - Canadian Human Rights Act	- Treasury Board Directive on Automated Decision-Making - Workplace health and safety obligations - Accessibility standards (Accessible Canada Act) - Cybersecurity guidance (CSE/CSEC) - Consumer protection and fair marketing laws
United States	- State privacy laws: CCPA/CPRA (California), CPA (Colorado), VCDPA (Virginia), CTDPA, UCPA - FTC Act (unfair or deceptive AI practices) - EEOC guidance on algorithmic hiring bias - Sectoral laws (HIPAA, GLBA)	- SEC governance expectations for listed firms - Algorithmic hiring requirements (e.g., NYC Local Law 144) - Cybersecurity obligations (NIST, CISA) - Consumer protection and advertising standards - NIST AI Risk Management Framework
Bermuda	- Personal Information Protection Act 2016 (PIPA) - Electronic Transactions Act 1999 - Human Rights Act 1981 - Employment Act 2000	- BMA conduct and governance rules for regulated sectors - Cybersecurity Code of Conduct - Ethical expectations for automated decision-making in regulated industries - Governance requirements under the Companies Act 1981
United Kingdom	- UK GDPR - Data Protection Act 2018 - Equality Act 2010 - Consumer Rights Act 2015 - Online Safety Act 2023	- ICO guidance on AI and data protection - UK AI Code (*to be published in 2026*) - Algorithmic transparency guidance (Cabinet Office) - National Cyber Security Centre guidance on AI and cyber security - UK ASA's Advertising Codes (CAP Code & BCAP Code)
Europe (EU)	- EU GDPR - EU AI Act (risk-based obligations) - Digital Services Act / Digital Markets Act - Charter of Fundamental Rights of the EU - EU Consumer Rights Directive	- NIS2 cybersecurity requirements - Worker consultation rights - Sustainability & reporting obligations under CSRD

[4] This is not an exhaustive list of the legal, regulatory and governance frameworks that organisations in these locations should consider when using AI systems in their operations. **Organisations should obtain legal advice to understand their compliance requirements in advance of AI deployment.**