

Artificial Intelligence (AI)
**Framework
and Policy**



Table of Contents

1. Introduction	3
2. Purpose and Scope	3
3. Definitions	3
4. Policy Statements	3
5. Key Processes	4
5.1 Risk Identification and Assessment	4
5.2 Data Classification and Usage	5
5.3 Implementation and Compliance	5
5.4 Disclosure of AI Usage	6
5.5 Accountability	6
6. Reporting	6
7. Controls	7
8. Related Policies	7
9. Policy Review	7
10. Document History	7
11. Appendix 1 – Detailed Example	8

Version #	1.0
Policy Owner	[Insert Policy Owner here]

1. Introduction

Artificial Intelligence (AI) is becoming integral to many business operations, offering opportunities for automation, insights, and efficiency. However, the use of AI also brings challenges and risks that must be managed carefully. This policy establishes a framework to guide the safe, compliant, and ethical integration of AI technologies in business processes. Some of the key processes outlined in this policy may be considered when implementing AI systems. Depending on the complexity and maturity of your business, not all processes may be necessary, and the level of detail may vary. This policy template provides a generic framework that can be adapted to fit the specific needs of your organisation.

2. Purpose and Scope

The purpose of this policy is to provide guidance on the principles and processes that should be considered when implementing AI systems within the organisation. It is designed to ensure that AI technologies are integrated responsibly, addressing legal, ethical, and operational considerations. This policy serves as a flexible framework that can be adapted to the specific needs of your business, depending on its complexity and maturity. It applies to all AI tools, models, and platforms used within the organisation, as well as the data and systems they interact with.

3. Definitions

Term	Definition
Artificial Intelligence (AI)	Technology that mimics human intelligence by enabling machines to learn, reason, and make decisions.
AI System	Any technology solution that employs AI algorithms, including machine learning models, predictive analytics tools, and decision-support systems.
Machine Learning (ML)	A subset of AI that uses data to train algorithms, allowing them to make predictions or decisions without being explicitly programmed.
AI Governance	A framework that oversees the ethical, legal, and technical management of AI systems.
Data Integrity	The accuracy, completeness, and consistency of data used in AI systems.
Bias	The unfair or discriminatory outcomes produced by an AI system due to flawed data, design, or assumptions.
Ethics	Principles of fairness, accountability, transparency, and responsibility as they relate to the use of AI.

4. Policy Statements

- Purpose of AI Usage:** The business uses AI technologies to assist with tasks such as content creation, process automation, and customer interactions. These AI tools are designed to improve efficiency and support decision-making while adhering to the company's standards of accuracy, fairness, and transparency.

- **Data Sensitivity and Protection:** AI systems used within the business will only process data that is appropriate for the intended task. Personal data, proprietary business data, and other sensitive information will only be used with proper legal grounds and protections, such as anonymisation or encryption, where necessary. AI tools must comply with all applicable data protection laws, including GDPR and industry-specific regulations.
- **Risk Assessment:** All AI systems must undergo a risk assessment before being implemented. This includes evaluating the type of data the system processes, identifying potential biases, and ensuring compliance with relevant regulatory frameworks. AI systems will be classified as low, medium, or high risk based on their impact on the business.
- **Data Input and Usage Governance:** Staff are required to follow strict guidelines when inputting data into AI systems. Only authorised personnel may input personal, proprietary, or sensitive data into AI tools, and explicit consent must be obtained where applicable. Data must be accurate, up-to-date, and ethically sourced to ensure the AI system generates reliable outputs.
- **Accountability for Deliverables:** Users are responsible for verifying the accuracy, appropriateness, and legality of all AI-generated outputs before incorporating them into final deliverables. While AI tools can assist with tasks, employees remain fully accountable for the final work product, ensuring it aligns with the company's standards and expectations.
- **Transparency and Disclosure:** The business will disclose when AI technologies have been used to generate content or interact with customers. This includes adding a note to public-facing content or customer service interactions where AI tools have been used, ensuring transparency and trust with stakeholders.

5. Key Processes

5.1 Risk Identification and Assessment

The first step in using AI is to assess the scope and potential impact of the AI tools being used. The risks involved may be less about critical decision-making and more focused on the ethical use of data for tasks like automating reports, creating policies, or supporting customer interactions.

- **AI Inventory:** Create a simple inventory of all AI tools in use. This might include text generation tools (e.g., for policy writing), chatbots, or content management systems that use AI to improve efficiency. For each, document:
 - the tool's purpose (e.g., content creation or automating responses).
 - the type of data it uses (personal data, proprietary business data, etc.).
- **Risk Assessment Framework:** Develop a framework to evaluate AI risks, focusing on:
 - **Data Sensitivity:** Evaluate the type of data being processed and ensure the data used by AI is appropriate (e.g., ensuring that sensitive personal data is not used).
 - **Potential Bias:** Even for simpler tools, businesses should check for bias, particularly in generated content or customer interaction tools.
 - **Regulatory Impact:** Review how the system complies with data protection laws, such as the General Data Protection Regulation (GDPR), and whether it meets industry-specific regulatory standards.

- **Risk Classification:** Based on the assessment, classify tools as low, medium, or high risk. For example, an AI tool used for internal document drafting might be low risk, while a chatbot that interacts with customers using personal information could be medium risk.

5.2 Data Classification and Usage

To ensure proper use of data, especially when AI tools are used to support tasks like content creation or customer interaction, staff must be given clear guidance on what information can be inputted into AI systems.

- **Data Identification:** Clearly identify what types of data the AI will process. If using AI for writing or content creation, the data may be less sensitive (e.g., general business information), but personal or proprietary business data (e.g., customer details, financial records, scorecards) must be handled carefully.
- **Guidance for Staff on Inputting Data into AI Systems:** Provide clear instructions to staff on what data can be input into AI tools:
 - **Do's:** Input general business information, product descriptions, and publicly available data. Use company proprietary information only if necessary and ensure it is protected (e.g., anonymize or encrypt proprietary data when possible).
 - **Don'ts:** Avoid using personal data (e.g., customer details, employee information) or sensitive company proprietary information (e.g., financial data, trade secrets) unless explicit consent is given and legal protections are in place.
- **Data Source Transparency:** If the AI tool uses third-party data or APIs, ensure that the data is sourced ethically, and if personal data is involved, appropriate permissions or consents are obtained.
- **Data Usage Governance:** Set clear rules for data usage within AI systems:
 - Ensure personal or proprietary data is not used without explicit consent.
 - Restrict who can input sensitive or proprietary data into AI systems to authorised staff only.

5.3 Implementation and Compliance

AI tools must be integrated in a way that complies with laws and ethical guidelines, even if the tools are relatively simple.

- **Data Governance:** Implement basic data governance processes. Ensure only authorised staff have access to data fed into AI tools, particularly when sensitive information is involved.
 - **Data anonymisation or pseudonymisation:** If personal data must be used, anonymise or pseudonymise it to protect privacy.
 - **Consent management:** If using personal data (e.g., for customer-facing AI tools), ensure that proper consents are in place.
- **Ethical AI Design:** Even with simple AI tools, ensure transparency and fairness:
 - **Fairness:** Ensure that the AI-generated outputs (e.g., policy drafts, chatbot responses) are free from bias.
 - **Transparency:** Make sure users understand what the AI tool does and what data it uses, particularly when interacting with customers.

- **Pre-deployment Testing:** Before fully implementing the AI, test its functionality and performance, ensuring that the results meet expectations. For instance, a content generation AI should be tested to ensure it produces relevant, accurate, and unbiased outputs.

5.4 Disclosure of AI Usage

For transparency and trust-building, the company must disclose when AI tools are used to generate public-facing content. This ensures that customers or stakeholders are aware of the role AI plays in generating the material they interact with.

- **AI-generated Content Disclosure:** Where applicable, disclose that AI tools were used to create or assist in the creation of certain content (e.g., blog posts, newsletters, or customer service responses). This disclosure may be included in a small note within the content or in a section of the company’s website.
- **Customer-facing Interactions:** If chatbots or AI-driven systems are used to interact with customers, clearly indicate that the responses are AI-generated, giving users the option to interact with a human if needed.

5.5 Accountability

While AI technologies are used to assist employees in their daily work, users remain accountable for the deliverables produced with AI assistance.

- **Responsibility for Output:** Users are responsible for verifying all AI-generated outputs before incorporating them into work deliverables. It is important to recognise that AI technologies may produce inaccurate, misleading, or outdated information.
- **Copyright Considerations:** Users must be mindful of copyright infringement when using data or information generated by AI technologies. Any content or data generated by AI tools must be properly vetted to ensure it does not infringe on the rights of third parties.
- **Human Oversight:** Users should maintain human oversight when reviewing AI outputs and be prepared to correct or adjust AI-generated content to ensure it meets the company’s standards and expectations.

Appendix 1 provides an example of how this process may be implemented in a business.

6. Reporting

Report	Description and Responsibilities
AI System Reports	Regularly report AI system performance, compliance status, and any issues related to data use to the executive team.
Incident Reporting	Any incidents involving the misuse of data, privacy violations, or biased AI outcomes must be reported immediately to the compliance team.
Data Usage Reporting	Provide periodic reports on how data is used within AI systems to ensure ongoing transparency and accountability.

7. Controls

Key Controls	How Implemented
Data Integrity Controls	Implement strict validation checks to ensure that only authorised and high-quality data is fed into AI systems. This includes measures to verify data accuracy and prevent the use of incomplete or outdated information.
Access Controls	Restrict access to sensitive or personal data, ensuring that only authorised staff can interact with data inputs to AI systems.
Audit Trails	Maintain comprehensive logs of data usage and AI decision-making processes, ensuring full traceability of how data impacts AI outcomes.
AI Governance Committee	Establish an internal review board responsible for approving AI systems and the data used, particularly for high-risk applications. This committee will oversee ethical, legal, and operational compliance.

8. Related Policies

Related Policies and Procedures
Privacy Policy
Information Technology (IT) Policy

9. Policy Review

This Policy shall be reviewed every year by [insert job title here].

10. Document History

Version Number	Date	Changes	Reviewed by	Date Approved by Board
1.0	October 2024	Draft Policy		

Next review date: October 2026.

11. Appendix 1 – Detailed Example

We may implement an AI-powered tool to generate marketing content for our social media channels and website. The AI assists in writing posts, blogs, or even drafting email newsletters based on inputted product information, audience details, and brand tone. Here's how the key processes in the policy would work in practice:

1. Risk Identification:

The business identifies that the AI system is low to medium risk because:

- The AI assists in content creation, but it is not making high-stakes decisions or handling sensitive personal data (e.g., it is not involved in customer billing or processing confidential business information).
- The primary risk is related to the content's appropriateness (e.g., avoiding bias, ensuring alignment with the brand, and ensuring no infringement on ethical standards).

2. Data Classification and Usage:

Before using the AI system, the business establishes what kind of data can be fed into it:

- **Data Identification:** The business determines that the AI can only use general business data like product descriptions, customer demographics (e.g., interests and purchase behaviors), and historical marketing materials. The AI does not use personal data unless it is anonymized (e.g., demographic trends without individual customer identities).
- **Data Source Transparency:** The business ensures the data input (e.g., product descriptions and previous campaigns) is owned by the business or obtained with permission (e.g., licensed stock descriptions).
- **Data Accuracy and Integrity:** The marketing team checks that all data fed into the AI is accurate and current (e.g., no outdated product descriptions or incorrect price points). This ensures the AI generates relevant and accurate content.

3. Implementation and Compliance:

The business follows basic implementation steps to ensure ethical and compliant use of AI:

- **Ethical AI Design:** The business instructs the AI to generate content that aligns with the brand's values and tone, ensuring it avoids content that might be offensive, biased, or misleading. For instance, if the AI generates posts about fitness products, the business ensures that it avoids body shaming or language that could be interpreted as discriminatory.
- **Pre-deployment Testing:** Before going live with AI-generated content, the business tests it by generating a few example blog posts or social media captions. The marketing team reviews these outputs to check for accuracy, relevance, and tone. For example, the business verifies that the content aligns with their brand voice (e.g., playful but professional) and avoids inappropriate suggestions.

4. Disclosure of AI Usage:

To maintain transparency and trust, the company discloses when AI tools are used to generate public-facing content:

- **Public Disclosure:** When applicable, the company will indicate that some content (e.g., blog posts or social media updates) has been generated or assisted by AI. This can be disclosed via a small note at the bottom of the content or through a general notice on the website.

5. **Accountability**

Although AI tools are used to assist with content creation, users remain accountable for the final deliverables:

- **Verification of AI Outputs:** Users are responsible for verifying all AI-generated content before publishing or incorporating it into work deliverables. It is important to note that AI technologies may produce inaccurate, misleading, or outdated information, and it is the user's duty to ensure that all outputs meet the company's standards.
- **Final Deliverable Responsibility:** The marketing team must review and take ownership of any content generated by AI, ensuring that it aligns with the company's brand, values, and accuracy expectations.
- **Copyright Considerations:** Users must also be mindful of potential copyright infringement. Any data or content generated by AI must be vetted to ensure compliance with copyright laws and respect for third-party intellectual property.