

Organizational AI Policy

Introduction

Artificial intelligence is becoming part of everyday work across many organizations. Staff may use AI to draft and summarize documents, analyze information, prepare presentations, translate content, generate ideas, automate routine tasks, or support decision-making.

In many cases, this adoption has happened quickly and informally. Employees may already be experimenting with AI tools before their organization has decided which tools are appropriate, what information can be shared with them, or what safeguards should apply.

An organizational AI policy provides a shared framework for using AI responsibly. It does not need to prevent experimentation or make AI difficult to use. Instead, it should help people understand where AI can add value, where the risks lie, and the boundaries they are expected to work within.

Why does your organization need an AI policy?

AI introduces questions that are not always fully addressed by existing IT, data protection, HR, or information security policies.

For example, an employee might paste part of a confidential report into an AI assistant to ask for a summary, upload a spreadsheet for analysis, use AI-generated research in a proposal, or rely on an AI tool to help assess applications. Each of these activities creates different considerations around privacy, confidentiality, accuracy, fairness, security, and accountability.

Without organizational guidance, individual employees are left to make these decisions themselves. Different teams may develop very different practices, and senior leaders may have limited visibility into which tools are being used or what information is being shared with them.

A clear AI policy establishes a consistent organizational position. It can explain which tools are approved, what employees may use them for, what information must be protected, when human review is required, and where employees should go when they are unsure.

Importantly, developing an AI policy is not simply about controlling risk. Clear guidance can also make responsible AI adoption easier. Employees who understand the boundaries are better placed to experiment confidently and identify useful applications for AI.

Organizational AI Policy

What are the risks of not having an AI policy?

The absence of a policy does not necessarily mean the absence of AI use. It may simply mean that AI is being used without consistent organizational oversight.

Without clear guidance...	The organization may face...
Employees select and use their own AI tools	Data may be shared with platforms that have not been assessed for security, privacy, or contractual risks.
Staff do not know what information can be entered into AI systems	Personal, confidential, financial, client, partner, employee, or other protected information may be exposed.
AI-generated information is not consistently reviewed	Incorrect, incomplete, fabricated, or biased information may find its way into organizational work.
There are no boundaries around AI-supported decisions	AI may influence decisions affecting people without sufficient human judgment or oversight.
New AI tools are adopted without a review process	The organization may take on security, legal, privacy, intellectual property, licensing, or financial risks.
Responsibilities are unclear	Employees may not know who is accountable for checking AI-generated work or addressing problems.
Staff are uncertain whether AI use is permitted	AI use may become hidden or inconsistent, reducing the organization's ability to understand how the technology is being used.

Organizational AI Policy

What should an organizational AI policy include?

There is no single policy that will work for every organization. The appropriate level of detail will depend on the organization's work, the information it holds, the people it serves, applicable laws and regulations, and how extensively AI is being used.

However, most organizational AI policies should address the following areas.

1. Purpose and scope

Start by explaining why the policy exists and who it applies to. This might include employees, consultants, contractors, volunteers, board members, or others using AI on behalf of the organization. The policy should also sit alongside existing organizational requirements rather than replacing them. Depending on the organization, this could include policies covering:

- Data protection and privacy
- Information and cybersecurity
- Acceptable use of IT
- Safeguarding
- Confidentiality
- Intellectual property
- Procurement
- Human resources

2. The organization's approach to AI

The policy should establish the organization's overall position on AI. For many organizations, this will mean recognizing the potential for AI to improve efficiency, support creativity, analyze information, automate routine tasks, and help employees work in new ways, while making clear that AI must be used responsibly, securely, and consistently with organizational values.

This section of an AI policy is an opportunity to establish principles that can continue to apply even as individual technologies change.

3. Roles and responsibilities

Responsible AI use is a shared responsibility so the policy should explain what the organization is responsible for, such as selecting appropriate tools, protecting organizational data, providing guidance and training, and monitoring AI-related risks. It should also establish expectations for leaders and managers, including helping their teams understand the policy, encouraging responsible experimentation, addressing concerns, and ensuring that appropriate oversight is maintained.

Finally, it should make clear what individual users are expected to do. This might include using approved tools, protecting sensitive information, reviewing AI-generated outputs, following relevant organizational policies, and reporting concerns or incidents.

Organizational AI Policy

4. Approved AI tools

Employees should be able to identify which AI tools are approved for organizational use. Approval should not necessarily mean that every type of information can be entered into a tool. Some platforms may be approved for general use but not for confidential or personal information, while enterprise tools with additional security and contractual protections may allow different uses.

Organizations should therefore consider documenting both which tools are approved and the conditions attached to their use. The policy should also explain what employees should do if they want to use an AI tool that has not yet been approved.

5. Data protection, privacy, and confidentiality

AI tools can make it extremely easy to share large amounts of information with an external system. Employees therefore need clear guidance about what information can and cannot be entered, pasted, uploaded, or otherwise shared.

Depending on the organization and the AI tools available, restrictions may apply to:

- Personally identifiable information
- Employee or payroll information
- Financial and banking information
- Confidential organizational information
- Client, member, donor, or partner information
- Safeguarding information
- Commercially sensitive information
- Proprietary or copyrighted material

The policy should distinguish between approved secure systems and public or unapproved AI platforms where appropriate. It should also explain when information needs to be anonymized before it can be used with AI.

6. Acceptable and prohibited use

Employees need practical examples of what responsible AI use looks like. Acceptable uses might include drafting or improving content, brainstorming ideas, summarizing appropriate documents, analyzing anonymized information, helping structure information, supporting translation, or automating routine administrative tasks.

Restrictions may be needed where AI is being used with sensitive information, to make high-impact decisions, or in circumstances where an AI-generated output could create significant consequences if it is wrong. Examples are particularly valuable here. A policy is easier to apply when employees can recognize situations from their own work rather than having to interpret broad principles.

Organizational AI Policy

7. Human review and accountability

AI-generated information should not automatically be assumed to be accurate, complete, unbiased, or appropriate. The policy should make it clear that people remain accountable for the work they produce or the decisions they make with AI support. Employees should review and, where necessary, verify AI-generated outputs before relying on, sharing, or publishing them.

Additional safeguards may be appropriate when AI contributes to decisions affecting individuals, including decisions relating to recruitment, employment, funding, procurement, safeguarding, or access to services.

8. Fairness, bias, and inclusion

AI systems can reproduce or amplify biases present in their training data, design, or the information provided to them. Employees should be expected to consider whether AI-generated outputs contain biased assumptions, discriminatory recommendations, stereotypes, inappropriate language, or a lack of cultural context. Human judgment is particularly important where AI outputs could affect people or communities.

9. Reporting concerns and incidents

The policy should tell employees what to do when something goes wrong. This could include accidentally sharing protected information with an AI system, discovering inaccurate or discriminatory outputs, identifying inappropriate AI use, or becoming aware of a potential privacy or security breach. Employees should know who to contact and should be encouraged to raise concerns promptly.

10. Training and support

A policy alone will not create responsible AI use. Organizations should provide appropriate training and guidance so employees understand both the opportunities and limitations of AI. Employees should also know where to go when they are uncertain whether a particular tool or use is appropriate. Training should evolve alongside the organization's use of AI rather than being treated as a one-time activity.

11. Assessing and approving new AI tools

AI tools should be reviewed before they are adopted for organizational use. The assessment should be proportionate to the intended use and the information involved, but organizations may want to consider the following areas (see next page).

Organizational AI Policy

Area	Questions to consider
Purpose	What will the tool be used for? What problem does it solve?
Benefits	How could it improve efficiency, quality, accessibility, or outcomes?
Data	What information will users enter or upload?
Privacy and security	How does the provider store, process, share, and protect data?
Confidentiality	Could organizational, employee, client, partner, or other confidential information be exposed?
Legal and compliance	Does its use meet relevant data protection, regulatory, and contractual requirements?
Bias and ethics	Are there known limitations or risks relating to bias or discrimination?
Reliability	Is the provider reputable, and are there known security or reliability concerns?
Intellectual property	What do the provider's terms say about inputs, outputs, ownership, and use of submitted content?
Cost and sustainability	Is the tool affordable and appropriate for ongoing organizational use?

Once a tool has been assessed, the decision should be documented. Approved tools should be added to the organization's approved tools list together with any restrictions or conditions of use. Where a tool is not approved, employees should understand why and, where possible, what alternatives are available.

Organizational AI Policy

Keep the policy under review

An AI policy should be treated as a living organizational document. AI technologies, their capabilities, provider terms, organizational use cases, and the regulatory environment are changing rapidly. A policy that accurately reflects an organization's AI environment today may not do so a year from now. Organizations should establish a regular review cycle for the policy, with a formal review **at least annually**. A review may also be needed sooner when:

- A significant new AI tool or capability is introduced
- The organization changes how it uses AI
- Relevant legislation, regulation, or guidance changes
- An AI-related privacy, security, or safeguarding incident occurs
- A provider makes significant changes to its terms, security arrangements, or handling of data
- Monitoring identifies a new or emerging risk

Not every change requires the entire policy to be rewritten. Organizations may find it useful to keep frequently changing information, such as the approved AI tools register, separate from the main policy so that it can be updated more easily.

Practical resources and templates for you

You can use the downloadable resources below to put this guidance into practice. The **Organizational AI Use Policy Template** provides a starting point for developing or updating your organization's policy, while the **AI Tool Request and Approval Form Template** supports a consistent process for assessing new tools before they are introduced. The **Approved AI Tools Register Template** can then be used to maintain a clear record of approved tools, their permitted uses, any restrictions, and when they are due for review. Download and adapt each resource to reflect your organization's context, existing policies, and approach to AI.

[Click here to download the Organizational AI Use Policy Template](#)

[Click here to download the AI Tool Request and Approval Form Template](#)

[Click here to download the Approved AI Tools Register Template](#)