

INTRODUCTION

As the adoption of artificial intelligence (AI) in the corporate world continues to grow, we recognise its potential to transform the way our members work and to improve their services and competitiveness. This guide has been developed to assist BESA members in creating an AI policy that ensures that AI tools are used and deployed securely and responsibly in the workplace. It sets out the key elements of an AI policy using the headings and wording below which you can adapt for your company.

1. Policy statement

Your AI policy should commence with a policy statement which is a declaration of your company's intention and commitment to ensure the ethical, secure and responsible use of AI in the workplace. An example of a policy statement is as follows:

"We are committed to ensuring that we use artificial intelligence (AI) responsibly, ethically, and lawfully. AI tools must be used in a way that protects confidentiality, respects privacy and intellectual property rights, avoids bias, and supports fair, transparent, and accountable decision-making."

"This AI policy establishes clear guidelines for the proper use of AI tools within our organisation. You are expected to read, understand and comply with these guidelines."

2. Scope of the policy

Your AI policy should identify who the policy applies to so that no individual can reasonably assume it does not apply to them.

The policy will typically apply to every individual employed by your company, including part-time, full-time, and temporary staff (together referred to as 'staff') during and outside normal hours of work and whether or not the use of AI is on the staff's own device or one of your company's devices, and whether at home, in the office or from a remote working location, provided it is for work purposes.

3. Definition of AI

Another crucial element of an AI policy is the definition of AI. A clear definition will clarify, and enable your staff to identify, what counts as an AI tool even when they are embedded in everyday software. It will also help your staff to understand the functionalities of these AI tools.

Broadly speaking, AI is a tool which simulates human intelligence in machines, generally computer systems. AI tools can learn, problem-solve, make decisions and understand language without human intervention. AI tools are generally trained on enormous banks of existing content from various sources called datasets. They then learn to identify patterns and relationships within these datasets to generate new content. More advanced AI tools can identify these patterns without human intervention or supervision, and self-train using additional prompt data and feedback from users. These functionalities highlight why you must consider the ethical, legal, and operational implications when deploying AI in the workplace.

4. Potential benefits of using AI in the workplace

It is vital for your AI policy to identify the potential benefits of using AI in the workplace. Understanding the benefits will encourage your staff to use AI tools in accordance with the policy rather than avoid them entirely. Some of the potential benefits are:

- They can be efficient tools for producing text, images or code quickly and to a specification. They aid efficiencies, e.g., *when used in brainstorming ideas, creating a first draft of or making transient, internal content.*
- They have the potential to improve productivity, personalise the customer experience and accelerate product/service developments. They may be capable of completing repetitive, manual high-volume tasks, and freeing up your staff for more relevant value-added work.

5. Potential risks of using AI in the workplace

Similarly, your AI policy should identify the potential risks of using AI in the workplace. This will tell the staff what can go wrong if they do not use AI tools responsibly. Some of the potential risks include:

a) Privacy and confidentiality

AI tools can exacerbate personal data and privacy risks. Unless specific consent is obtained, entering personal data into a publicly accessible AI tool (which can store the information indefinitely, recycle and reuse it) is likely to constitute a data protection breach under the data protection law. Using publicly accessible AI tools also runs the risk of exposing your (proprietary) information, and breaching your duty of confidentiality, where applicable.

b) Intellectual property (IP) and trade secrets

AI tools can increase the risk that your company's IP (such as our logos and trade names) and trade secrets will be improperly disclosed. Most publicly accessible AI tools do not guarantee the information

you input into the tool will not be used to train the AI model. This means your IP could be reproduced or made available to other users in some form.

Inputting third-party information into an AI tool without proper licence may infringe IP owned by third parties. This could be information belonging to your customer, supplier or party completely unconnected to your operations.

c) Accuracy

The output of an AI tool may not be guaranteed to be 100% accurate. For example, where AI does not have the data to provide the information you have requested, it may still attempt to produce an output by simply making things up (also known as “hallucinations”). Relying on a response or text produced from an AI tool without checking could have a range of negative outcomes, including damage to your reputation.

d) Bias

There is the potential for bias to be embedded within the AI tool, from the data used to train the AI tool or the coded instructions that tell the AI tool how to function. This bias can then be perpetuated as the AI tool operates and develops, inadvertently leading to the creation of discriminatory content or decisions. This is not necessarily deliberate; the AI tool may simply be reflecting the unconscious bias of its creators or other users.

e) Increased risk of data breaches

AI tools can aggravate the risk of data breaches. They are high-value targets for cyberattacks because they store vast amounts of sensitive data from multiple organisations. If an AI vendor (e.g., Microsoft Co-pilot) suffers a breach, your confidential information could be exposed, leading to severe financial, legal, and reputational consequences.

Third-party breaches typically carry a higher cost than internal breaches. Once data leaves your environment, you lose visibility and control, making it more difficult to determine what was compromised, respond promptly, or meet regulatory obligations should a breach occur.

6. Approved AI tools and who may use them

Your AI policy should specify the AI tools approved by your company so that your staff can know exactly which tools they may use for work and the company can implement appropriate compliance controls. You may also provide for training sessions on the use of the approved AI tools. The policy should also state that any additional AI tool must be vetted and approved by *[insert the team/person responsible]* before use.

Additionally, your policy should stipulate who may use the AI tools and how they may use them. For example, *“All staff are permitted to use the approved AI tools in accordance with this policy, all applicable laws (including data protection and privacy laws) and other relevant internal policies.”*

7. Guidelines for staff on using AI tools and platforms

Very importantly, your AI policy should specify the guidelines for use of the approved AI tools. Some of our recommended guidelines include:

- You must not use any unapproved AI tool in carrying out your work. If you wish to use another AI tool, you should contact the *[insert the team/person responsible]* to ask whether the AI tool can be approved under this policy and/or whether you can be given authorisation to use it.
- When using any approved AI tool in the workplace, you must always use your company email address to create and log in to the approved AI account and protect your login credentials.
- You must not share your access or login credentials or allow others to use the approved AI tools on your behalf.
- You must not use the AI tools in any way that could be considered discriminatory, or could give rise to defamation, harassment, intimidation or bullying or in any way that could harm the reputation of another.
- You must not use the AI tools to create illegal content or for illegal purposes.
- You must not use offensive, obscene or abusive language, graphics or imagery when inputting content into the approved AI tools and must not attempt to create content which is offensive, obscene or abusive through your use of the approved AI tools.
- You must not input into any unapproved and publicly accessible AI tool:
 - (a) the company's trademarks, brands, logos or any other identifying material;
 - (b) any of the company's name, email or other contact details;
 - (c) proprietary company information;
 - (d) customer or supplier materials, information or data;
 - (e) trade secrets, confidential or valuable information;
 - (f) usernames, passwords (other than for the AI tool itself), and security tokens; or
 - (g) personal data.
- You must not in any way provide or suggest any endorsement or recommendation by the company of any unapproved AI technology.
- Your use of AI tools in the workplace must be limited to work-related purposes.
- You are responsible for ensuring the generated content aligns with the company's values, ethics and quality standards.
- Before using any AI generated content (except for AI generated images, videos, voice recordings, trademarks and logos), you must carefully review it and ensure you do not use content that:
 - (a) discloses confidential, proprietary company information or personal data without approval from your line manager;

- (b) has the potential to breach the intellectual property rights of a third-party;
 - (c) is misleading and/or cannot be verified; and
 - (d) is discriminatory, otherwise biased or offensive.
- You must not use any AI generated image, video, voice recording, trademark or logo for work-related purposes without prior approval from the *[insert team/person responsible]*.
 - You must comply with the terms and conditions of the AI technology that you use, unless such terms and conditions conflict with or contradict the company's policies or your terms of employment, in which case you should seek advice from the *[insert team/person responsible]*.
 - You must report any AI-related incidents, near misses, suspected misuse and breach of this policy immediately to your line manager in the first instance.

8. Responsibility for compliance

The staff and team which are responsible for ensuring compliance should be recognised in the AI policy. Ideally,

- All staff are responsible for ensuring their own use of AI tools is in accordance with the policy and must make themselves aware of, and comply with, their responsibilities, as outlined in the policy, to protect confidential and sensitive information when using AI.
- Managers and supervisors are responsible for ensuring their teams are aware of and comply with the policy and they must report any breach of this policy to the *[insert team/person responsible]*.
- The Human Resources team are responsible for handling any complaints concerning violation of or non-compliance with the policy, including any allegations of harassment, discrimination, or bias that may be raised by employees, members, customers, suppliers or other third parties.

9. Consequences of a breach of the policy

Your AI policy should state the consequences of a breach which may include disciplinary action and dismissal, depending on the nature and gravity of the breach. Stating the consequences of a breach will reinforce the importance of secure responsible use of AI, support the effective enforcement of the policy, and act as a deterrent by ensuring your staff understand that breaches will be addressed appropriately and proportionately.

10. Monitoring and review

Your AI policy should include a clause which states that the policy will be monitored and reviewed regularly. This will help to ensure that your policy is updated to reflect legal requirements, best practices and the continuous improvement of your use of AI.

Your reviews may be conducted at scheduled intervals and/or where triggered by relevant developments such changes in law or regulation, technological advancements, emerging risks, identified incidents, or material changes to the company's use of AI.

Please note: this factsheet was written in April 2026 and is intended for general information purposes and does not constitute legal or other professional advice. The information is considered to be correct at the time of publication however any changes and further developments may impact the accuracy and validity of the information provided here.