3.
Developing an AI Policy

3. Developing an AI Policy

An AI Policy is an essential governing document to mitigate legal and reputational risk in any organisation that is actively using AI technologies. Alongside managing risk, a well written and widely utilised policy also champions best practice and supports the adoption of technologies and workflows that can support an organisation to deliver on its mission and vision.

First Principles	Developing an AI Policy for your Organisation
Purpose and Scope • When developing an AI Policy, it is important to identify its scope. Your first policy does not need to cover all potential future uses of these technologies, nor does it need to be a definitive text. • Striving for perfection may prevent you from ever finalising or adopting an appropriate policy. Instead, taking an agile approach allows you to support existing good practice and mitigate current risks within your organisation. • The policy can grow and develop in line with the adoption and development of these technologies. • The policy should address current use of AI technologies in your organisation, support and champion good practice and mitigate the risk of practices that are not aligned with the organisations values, and UK GDPR. • Artificial Intelligence is a broad term that covers a wide range of advanced technologies. Be clear about what your policy covers. If your policy is focussed on the use of Generative AI, state that. • Explain what Generative AI technologies are, how they work, and which platforms use this technology. Consider your organisations mission and values, align the AI Policy accordingly.	Revisit the 'Starting the AI Conversation' Worksheet and use the data collected through that exercise to complete the first principles of your AI Policy. Each box invites you to draft a short statement that will serve as building block in your AI Policy.

Guiding Principles / Values • Your organisation's values will determine your appetite for risk, the types of platforms you permit staff to use, and approach to mitigating risk e.g. how you might consider the impact of AI's environmental impact.	
Acceptable and Prohibited Use • This section should build upon your guiding principles but take a more directive approach. • Outline existing acceptable uses of AI technologies in your organisation. • Explain how they are being used and reflect upon the mechanisms for human oversight. • Outline use cases that are not permitted and explain why (this may be a legal compliance or values-based decision).	
Tools and Compliance AI Platforms present both data and cyber security risks. Understanding what platforms staff are using and assessing them from a data protection and cyber security perspective can provide a central mechanism for managing what platforms are being used for your organisation's data. • Audit platforms currently being used and provide an overview of its compliance with UK GDPR. • Advise staff that all platforms present UK GDPR and cyber security risk. • Caution against any platform not explicitly listed in the policy as safe for use.	

Top Tips

A policy will only ever be as good as the level of adoption it receives. Starting a conversation about what AI means for your organisation is an excellent way to empower and onboard staff early, so that the adoption of an AI Policy is realised across the organisation.

There is no one-size-fits all AI Policy. The best way to begin developing an AI Policy is to speak with colleagues.

Once you have drafted the policy:

- Seek meaningful consultation with staff across the organisation.
- Incorporate feedback and refine the policy.

After adoption, establish a review period and expand the policy to address blind spots and emerging trends.