FUTUREPLUS

RESPONSIBLE & SUSTAINABLE AI USE GUIDE

INTRODUCTION

Artificial intelligence (AI) is increasingly embedded across business operations, including marketing, recruitment, customer service, analytics, software development, design, finance, and decision support. While AI offers significant opportunities for efficiency, innovation, and productivity, it also introduces environmental, ethical, operational, and governance risks that organisations must manage responsibly.

To listen to our bitesize podcast episode on responsible AI, click here.

This guide is for organisations using generative AI tools, machine learning systems, automated decision-support technologies, or AI-enabled software across their operations. It aims to provide practical guidance to help businesses move from informal or fragmented AI adoption toward more structured, transparent, fair, and sustainable AI governance, ensuring that AI systems are:

- Used transparently and ethically
- Governed with appropriate oversight
- Monitored for bias and unintended outcomes
- Applied proportionately based on risk
- Used in ways that protect privacy and confidentiality
- Used in ways that comply with legal and regulatory developments
- Considered within their full environmental and operational life cycle

UNDERSTANDING AI GOVERNANCE MATURITY

Organisations are often at different stages of AI adoption. Responsible AI governance should evolve alongside organisational use:

Level 1	Informal or ad hoc AI use with limited oversight
Level 2	Basic awareness training and initial guidance in place
Level 3	Formal AI policies and governance processes established
Level 4	AI risks, sustainability, privacy, and fairness integrated into operational governance
Level 5	Continuous monitoring, auditing, reporting, and improvement embedded across the organisation

This guide is designed to help organisations progress toward more mature and accountable AI practices.

IMPLEMENTING AN AI POLICY

An AI policy defines how artificial intelligence is approved, used, governed, monitored, and reviewed across an organisation. Without a clear policy, AI adoption often becomes fragmented across teams, leading to inconsistent practices, unmanaged risks, duplicated tools, data exposure, and unclear accountability.

We recommend that at a minimum, an AI policy should include:

- Approved (and prohibited) AI tools
- Rules for handling confidential or personal data
- Approval processes for new AI use cases
- Risk-based categorisation of AI applications
- Sustainability and efficiency considerations
- Human oversight requirements
- Accountability and ownership structures
- Review and audit processes

MAINTAINING AN AI USE REGISTER

We also recommend maintaining a simple AI use register to improve oversight and accountability. This will help leadership teams to understand:

- Which AI tools are being used
- Why they are being used
- What data is involved
- Which teams are responsible
- What level of oversight is required

DATA PRIVACY, CONFIDENTIALITY & SECURITY

AI systems can introduce significant privacy and confidentiality risks if used improperly.

Many public AI tools may retain prompts, inputs, or uploaded files for service improvement, model training, or logging purposes. Employees may unintentionally expose commercially sensitive, confidential, or personal information when interacting with unapproved tools.

Organisations should establish clear rules around what information can and cannot be entered into AI systems, handling of customer and employee data, third-party AI provider risks, as well as retention and deletion policies.

Good practices include:

- Prohibiting entry of confidential or personal data into unapproved AI systems
- Requiring legal or security review before adopting new AI tools
- Reviewing provider data handling practices
- Aligning AI use with GDPR and other applicable privacy regulations

TRAINING EMPLOYEES

Employee training is essential to ensure AI is used appropriately, safely, and efficiently across an organisation. Without adequate training, AI may be used excessively, inconsistently, or for tasks where it adds little meaningful value.

Effective training should help employees understand when AI is appropriate to use and when human judgement remains preferable, while also building awareness of how to avoid unnecessary or excessive prompting that increases operational and environmental impact. Employees should also be equipped to identify potentially biased, misleading, or inaccurate outputs, protect confidential and personal data appropriately, and use AI tools responsibly and proportionately within organisational policies and governance expectations.

Training should typically include:

- Responsible prompting practices
- Environmental and carbon awareness
- AI limitations and hallucinations
- Bias and fairness awareness
- Data protection and confidentiality requirements
- Human review obligations
- Organisational approval processes

WHY AI CAN HAVE BIAS

AI systems can produce biased outcomes because they learn from historical data, and that data often reflects existing social, economic, or organisational inequalities. The system does not understand fairness; it identifies patterns and reproduces them.

A common mechanism is inheriting bias from training data. If past decisions within an organisation were uneven or influenced by structural bias, the AI model trained on that data may learn to replicate those patterns. For example, if historical hiring data shows fewer women in senior technical roles, an AI recruitment system trained on that data may unintentionally rank male candidates more highly because it associates “success” with previous hiring patterns rather than objective capability.

Bias can also emerge in more subtle ways, such as:

- AI systems prioritising faster-resolving customer groups based on historical data, unintentionally disadvantaging more complex or vulnerable cases
- Recommendation systems reinforcing existing consumption patterns that exclude less represented groups

This is why AI bias is not a static issue but an ongoing governance concern that requires continuous monitoring and human review.

INFORMING STAKEHOLDERS WHEN AI IS USED IN MATERIAL WAYS

Organisations should be transparent when AI is used in ways that meaningfully influence outcomes experienced by customers, employees, users, or other stakeholders.

“Material use” generally means AI is actively shaping decisions, content, visibility, recommendations, prioritisation, or user experiences rather than simply operating as a background productivity tool.

AI use is likely material when it:

- Influences decisions affecting people
- Shapes customer access or visibility
- Produces external-facing communications
- Automates prioritisation or scoring
- Replaces tasks previously requiring human judgement
- Could reasonably affect trust, fairness, or outcomes

Transparency is vital because stakeholders may otherwise assume that human judgement was solely responsible for outcomes when AI systems have in fact played a significant role. Organisations can support transparency by clearly labelling AI-generated content, disclosing when recommendations or outputs are AI-assisted, notifying users when they are interacting with AI systems, and including clear statements about AI use within policies, privacy notices, or service documentation.

Where automated systems influence decisions, prioritisation, or access to services, organisations should also explain the role AI has played in those processes. Clear and transparent communication helps strengthen trust, accountability, and informed engagement with AI-enabled systems.

“HUMAN IN CONTROL” OVERSIGHT

A human-in-control approach ensures that AI does not act as the final decision-maker in high-impact scenarios. This is essential because AI systems do not understand context, lived experience, or ethical nuance, and may reproduce or amplify bias present in training data.

Human oversight is especially important in reviewing edge cases and vulnerable cases. These are situations where automated systems may struggle to interpret context correctly or where individuals fall outside typical data patterns. Humans are better able to apply judgement in these scenarios, ensuring that unusual or sensitive cases are treated fairly and appropriately rather than being misclassified or de-prioritised by algorithmic logic.

Oversight mechanisms typically include pre-decision human review, regular audits of AI outputs to identify bias, override systems that allow human correction, and feedback loops that improve future performance.

ENVIRONMENTAL CONSIDERATIONS

AI's operation relies on large-scale data centres that consume significant amounts of electricity and water for computational processing and cooling infrastructure, while also contributing to carbon emissions associated with energy use.

In addition, AI depends on resource-intensive semiconductor manufacturing, global hardware supply chains, and the extraction of raw materials such as rare earth metals. The rapid growth of AI is also expected to increase electronic waste as servers and computing hardware are replaced or upgraded.

However, the dominant source of emissions associated with AI is the *use* of AI itself, as opposed to the training or hardware manufacturing. Recent research indicates that inference (the process of running a model) now accounts for over 90% of the total lifecycle emissions of an AI system. While per-query emissions are relatively small, AI's footprint scales with usage (particularly with use of Agenic AI) and depends heavily on grid carbon intensity. In other words, the volume, frequency and efficiency of how your organisation uses AI models matters most.

Responsible AI governance should therefore include environmental sustainability considerations alongside ethics and operational risk, such as:

- Choosing appropriately sized models for business needs
- Reducing unnecessary repeated generation
- Improving workflow efficiency rather than maximising usage
- Extending hardware life cycles where appropriate
- Managing storage and data retention responsibly
- Making procurement a lever by reviewing vendor sustainability disclosures - look for:
    - Data centre region-level emissions factors
    - Market vs. location-based scope 2
    - A clear methodology for emissions estimates
    - Evidence of high quality renewable procurements (PAAs, not RECs)
    - Data centre efficiency improvements

NEED MORE HELP?

For more help from your Advisor, contact the team: info@future-plus.co.uk.

FuturePlus also offers consultancy and carbon accountancy services to support organisations in developing responsible and sustainable operational practices. Access our consultancy services here.