Artificial Intelligence Policy

Introduction

This policy sets out the principles and standards for the ethical and responsible use of Artificial Intelligence (AI) across Nviro.

This policy applies to all employees who use AI tools or systems in the course of their work. It includes any AI-assisted processes used for planning, communication, administration, data analysis, innovation, or service delivery. Contractors and partners are expected to respect Nviro's policy when utilising company data.

Policy Aim

It is designed to ensure that AI technologies are used in ways that are safe, transparent, ethical and beneficial to both our colleagues and clients. This includes the opportunity for automation, which means that vast amounts of information can be gathered and analysed quickly. We are committed to embracing technology so that we can continue to innovate and improve our organisation, but we are also highly aware of the risks that come with new technologies.

Ethical Principles

We are committed to using AI responsibly and in alignment with our company values. Our use of AI will be guided by the following ethical principles:

- **Transparency**: We will ensure that AI systems and their outputs are understandable and can be explained to those affected by their use. Outputs that have been AI generated will be labelled as such.
- **Fairness**: AI tools must not discriminate or reinforce bias, especially in relation to colleague management or customer service.
- **Accountability**: Humans will always remain responsible for key decisions. AI should support, not replace, professional judgment.
- **Privacy and Data Protection**: All AI use must comply with applicable data protection legislation, including the UK GDPR. Sensitive data must not be entered into unapproved AI platforms.
- **Wellbeing and Safety**: AI must enhance workplace safety and support employee wellbeing, never compromise it.

Acceptable Use Guidance

AI tools may be used in the following ways within the business:

✅ Examples of Appropriate Use:

- Drafting written communications, bid content, contract responses, reducing word counts, or marketing materials — provided final review and editing is completed by a person.
- Creating cleaning rotas, schedules, or resource plans based on fixed data inputs.
- Analysing trends in site audit results, feedback forms, or helpdesk tickets.
- Translating documents or communications, then checking accuracy before sharing.
- Using chatbots or AI tools to streamline internal admin or form filling.

- Carrying out research or benchmarking.

❌ Examples of Inappropriate Use:

- Uploading client names, addresses, or contract data into public AI tools like ChatGPT, Bard, or Copilot unless settings ensure privacy and data control.
- Relying on AI to make employment-related decisions, such as rejecting applicants or recommending disciplinary action.
- Using AI to impersonate individuals or automate responses that could be mistaken for a real person.
- Allowing AI-generated cleaning plans to go live without site validation or management approval.

Responsible Use and Risk Mitigation

To ensure AI is used safely and effectively:

- All AI-generated outputs must be reviewed and validated by a human before use or submission.
- New AI tools or systems must be approved by senior management before adoption.
- Any AI-generated videos for e-learning purposes must include a caption to explicitly state they have been generated using AI. Creation of AI avatars must only be done using approved suppliers who will also store appropriately.
- AI should augment human roles rather than replace them; automation must not compromise job quality or employment rights.
- AI should not replace any Quality Manual Process or pathway.
- Vendors or third-party AI tools must be vetted for data security, compliance, and ethical use.

Training and Awareness

To support responsible use of AI, we will:

- Provide staff with basic training on how to use approved AI tools appropriately. Specific training will be provided within individual job roles depending on the needs of the business and expanding use of AI.
- Raise awareness of the limitations and potential biases of AI systems.
- Ensure employees know how to escalate questions or concerns related to AI use.

Monitoring and Review

AI use across the business will be regularly monitored to ensure it remains ethical, secure, and effective. We will:

- Review AI applications annually, or more frequently if legislation or tools evolve.
- Collect feedback from staff and clients on the use of AI within our operations.
- Address any misuse or unintended consequences promptly.

Governance and Responsibility

Governance of this policy rests with the Finance Director, with the maintenance of the Approved AI Register the responsibility of the Asset and Supplier Manager. They are responsible for:

- Reviewing developments in AI relevant to our industry and operations.
- Advising on the safe and effective implementation of new tools.
- Ensuring that staff comply with this policy.

Practical Guidance for Using AI Tools

To protect sensitive information and ensure AI tools are used correctly, employees should follow these best practices:

🔒 Tool Settings and Data Controls:

- Use AI tools that offer enterprise or business accounts where possible - these typically do not train the model on your input data.
- **Disable data sharing or "Improve the model" settings** where available:
    - In ChatGPT: Turn off "Improve the model for everyone" in the settings, under "Data controls".
    - In Microsoft Copilot: Use under your work account with organisational data protections enabled.
    - In Google Gemini: Use in Incognito or ensure your input is not saved to your history.
- **Never** enter:
    - Client names, site addresses, contact details, or pricing information.
    - Staff personal data or employee issues.
    - Financial or legal content that has not been anonymised.

✅ When using AI:

- Label outputs clearly if AI-assisted (e.g., "Draft generated using AI, verified by [Your Name]").
- Cross-check facts, figures, and references against official sources or internal documents.

❌ Avoid:

- Copying and pasting sensitive email chains or policy documents into public AI platforms.
- Using unverified browser plugins or AI apps linked to your company accounts.
- Assuming AI-generated content is always accurate — it may produce false or misleading information.

Policy Review

This policy will be reviewed at least once per year and updated as required in line with changes to technology, legislation, or business practice.

Appendix A

Approved AI Tools Register

The following AI tools are approved for use by Nviro, provided they are used in conjunction with this policy:

- ChatGPT
- Microsoft Copilot
- Google Gemini
- Perplexity
- Gamma
- Adobe Acrobat AI Assistant
- Fireflies.ai Notetaker

Appendix 2 – Risk Review

Risk Review - AI			
Risk Category	**Description**	**Risk Level**	**Controls or Recommendations**
Data Privacy	Risk of personal or client data being entered into public AI tools and processed outside the UK/EU.	High	▪ Prohibit sensitive data entry into public tools (e.g. ChatGPT). ▪ Use business/enterprise AI tools. ▪ Disable “training” settings.
Inaccurate Outputs	AI-generated content may contain errors, hallucinations, or outdated information.	Medium	▪ All AI outputs must be reviewed and approved by staff. ▪ Never use AI for final legal or compliance content.
Bias and Discrimination	AI tools may produce biased outcomes, especially in recruitment or performance analysis.	Medium	▪ Prohibit AI use in automated decision-making for HR matters. ▪ Human review required for fairness and accuracy.
Reputation and Trust	Poor or incorrect use of AI may damage client trust or result in misleading content being shared.	Medium	▪ Introduce a staff policy and training on responsible use. ▪ Mark AI-generated content clearly and check for factuality.
Cybersecurity	Third-party AI platforms could introduce vulnerabilities or allow data leaks.	Medium	▪ Use only approved AI tools. ▪ Conduct vendor assessments for security compliance.

			▪ Apply multi-factor authentication where possible.
Job Displacement	Concerns among staff that AI will replace human jobs, particularly in admin or planning roles.	Low	▪ Position AI as a support tool, not a replacement. ▪ Communicate clearly and involve staff in digital change processes.
Compliance Risk	Breach of UK GDPR or failure to meet procurement/contractual standards through inappropriate AI use.	High	▪ Maintain human control over AI use in client tenders and reports. ▪ Provide data protection training with AI scenarios.
Overreliance	Risk of staff becoming overly dependent on AI, leading to skill loss or unchecked automation.	Medium	▪ Require manual review and sign-off on AI-generated outputs. ▪ Continue training and upskilling of team members.