AI acceptable use policy template

A short policy template setting out which AI tools staff may use, what data must never go into them, and who is accountable.

Replace everything in [square brackets]. Keep the policy short, and review it every six to twelve months as tools change.

1. Purpose

This policy explains how staff at [Organisation name] may use artificial intelligence tools safely, lawfully and productively, and protects the personal and confidential information we hold.

2. Scope

It applies to all staff, contractors and volunteers, and to all AI tools that generate text, images, code, audio or analysis, including tools built into other software.

3. Approved tools

Tool	Approved account type	Approved uses
[Tool name]	[Enterprise account]	[Drafting, summarising public documents]
[Tool name]		

Any other tool needs approval from [role] before use.

4. Information rules

- **Never** enter sensitive personal data, such as health, religious, ethnic or biometric data, or children's data.
- **Never** enter personal data about customers, beneficiaries, patients, students or staff into a tool that is not approved for it.
- **Never** enter passwords, security details, unreleased financial information or confidential contracts.
- **Remove or replace** identifying details before using approved tools where possible.

5. Quality and accountability

- Staff are responsible for checking AI output for accuracy, bias and suitability before using it.
- AI must not make final decisions about people without meaningful human review.
- Content published externally that was substantially produced with AI should be reviewed by [role].

6. New AI tools and projects

Before introducing a new AI tool or using AI on personal data, [role] will assess the privacy and security risks and, where needed, carry out a data protection impact assessment.

7. Training and reporting

All staff will receive AI awareness training. Report any mistake, such as personal data entered into an unapproved tool, to [name or role] immediately so it can be handled as a possible data breach.

8. Breaches of this policy

Breaches may lead to disciplinary action.

Policy owner: [role]. Approved by: [name]. Date: [date]. Next review: [date].

Free resource from SafeDaTech · safedatech.com · info@safedatech.com · 08165771517
General guidance only, not legal advice. Adapt it to your organisation. © 2026 EDAN Development & Consulting Ltd.