

AI Acceptable Use Policy

A ready-to-adapt policy template for small and mid-sized businesses. Replace the highlighted fields and make it yours.

Organisation	[Company name]
Policy owner	[Name, role, e.g. IT Manager]
Approved by	[Name, role]
Effective date	[Date]
Next review	[Date + 6 months]

1 • Purpose

AI tools can make our work faster and better. They can also expose confidential information, produce incorrect results, and be used by criminals to impersonate people we trust. This policy explains how [Company name] staff may use AI tools safely.

2 • Scope

This policy applies to all employees, contractors, interns and anyone else who works with [Company name] data or systems. It covers any AI tool used for work, on company or personal devices: chatbots, writing and coding assistants, image, audio and video generators, meeting transcription, AI features in existing software, browser extensions, and AI agents that can take actions.

3 • Definitions

- **AI tool:** software that uses AI to generate, summarise, analyse or act on content.
- **Approved AI tool:** a tool listed in section 4, used through the account type stated there.
- **Shadow AI:** an unapproved AI tool used for work, or an approved one used through a personal account.
- **Sensitive data:** anything classified as Confidential or Restricted in section 6.
- **AI agent:** an AI tool that can take actions, such as sending emails, editing files or changing systems.

• UNVERIFIED



```
> trust = 0; verify --all
```

How to use this template

1. Replace every **[highlighted]** field and delete what doesn't apply.
2. Fill in the **approved tools** table first. Without approved options, people turn to unapproved ones.
3. Have it reviewed by whoever handles **legal, HR and data protection** for you.
4. Brief staff and collect **signed acknowledgements** (page 4).
5. Review it **every 6 months**. AI tools change quickly.

Why it matters

In IBM's Cost of a Data Breach Report 2025, **1 in 5** organisations had a breach linked to shadow AI, high shadow-AI use added about **\$670,000** to the average breach cost, and **63%** had no AI governance policy.

General guidance, not legal advice. Need the editable Word version? Email info@alphatechs.al.

Why Alphatechs

24/7 security operations with a 30-minute response, penetration testing, and Sphere TI, our own threat intelligence platform.

Take the Next Step

Need help putting AI governance in place? Free 30-minute call: alphatechs.al/contact

4 · Approved AI tools

Only the tools below may be used for work, through the account type shown. Business accounts give us data protection terms, admin controls and the option to stop our data being used for model training.

Tool	Approved for	Account type	Highest data class
[e.g. company AI assistant]	[drafting, summarising, research]	[Business, company login]	[Internal]
[e.g. coding assistant]	[code in approved repositories]	[Business, SSO]	[Confidential: code only]
[e.g. meeting transcription]	[internal meetings, with notice]	[Business]	[Internal]
[Tool]	[Use]	[Account]	[Class]

Any tool not on this list is not approved. To request one, follow section 11.

5 · Rules for everyone

You must:

- Use only approved tools, signed in with your company account.
- Check that the data you enter is allowed for that tool (section 6). If in doubt, leave it out.
- Remove names, contact details and account numbers wherever the task allows.
- Review and take responsibility for any AI output before you use it.
- Report mistakes quickly (section 13).

You must never:

- Enter passwords, keys, tokens, one-time codes or other credentials.
- Enter Restricted data into any AI tool.
- Use personal AI accounts or free consumer versions for work.
- Install AI extensions, plug-ins or apps without IT approval.
- Connect AI to company email, files or systems without IT approval.
- Let AI make final decisions about people without human review.
- Create content that impersonates a real person or is misleading.

6 · What data can go into AI tools

Class	Examples	Allowed in approved AI tools?
Public	Published website text, press releases, public product information	Yes, in any approved tool
Internal	Internal procedures, non-sensitive emails, meeting notes, drafts	Yes, in tools rated Internal or higher
Confidential	Client names and contracts, pricing, financials, source code, strategy	Only in tools approved for Confidential data, and only what the task needs
Restricted	Personal data (IDs, health, HR, payroll), bank and card details, credentials, security configurations, privileged material	Never , unless the Policy Owner approves a specific tool and use in writing

7 · Accuracy and human review

AI tools can produce confident, well-written answers that are wrong, outdated or invented. You're responsible for the accuracy of anything you use.

- Check facts, figures, names, legal or technical statements and references against reliable sources.
- Have AI-generated code reviewed like any other code, including for security issues and licence obligations.
- Where customer-facing content is substantially AI-generated, follow [Company name]'s disclosure guidance: [describe].

8 · Intellectual property

- Don't enter third-party content we don't have the right to use, such as a client's confidential documents, unless the contract allows it.
- Don't present AI-generated work as original where that would mislead, and check for obvious copying before publishing.
- Work you create with AI tools for [Company name] is treated like any other work product.

9 · AI agents, extensions and integrations

Tools that can read our systems or take actions carry more risk, because hidden instructions in an email, document or web page ("prompt injection") can trick them into doing something harmful.

- Every agent, extension or integration needs IT approval before use.
- They get only the access their task needs, and access is reviewed [every 3 months].
- Anything that sends information outside the company, moves money, deletes data or changes security settings needs human approval.
- IT keeps a register of approved agents, extensions and integrations and what they can access.

10 · Security: AI-enabled scams and deepfakes

Criminals use AI to write flawless phishing, clone voices and fake video calls. So we trust nothing and verify everything:

- Requests to pay money, change bank details, share credentials or send sensitive data are **always verified through a second, known channel**, even if they seem to come from a manager on a video call.
- Payment verification follows [link to payment procedure], including dual approval above [amount].
- Suspicious messages, calls or AI outputs are reported to [security contact] immediately.

11 · Requesting a new AI tool

Send requests to [IT contact / form] with the tool and provider, what you want to use it for, what data it would need, and who else would use it. IT reviews data handling, security, contract terms and cost, and aims to respond within [10 working days].

12 · Training

Everyone covered by this policy completes AI-safety training when they join and [once a year] after that, covering this policy, safe prompting, data classification, output checking and AI-enabled scams. [Adjust to meet any AI-literacy obligations that apply to you, such as Article 4 of the EU AI Act.]

13 · Reporting incidents

Report to [security contact] within [1 hour] if you:

- entered Confidential or Restricted data into a tool where it wasn't allowed;
- used an AI tool that turned out to be malicious or not what it claimed;
- notice an AI tool or agent behaving unexpectedly, or taking actions you didn't ask for;
- receive a request you suspect is AI-generated impersonation.

Reporting quickly and honestly is never treated as misconduct. Delays make the impact worse and can mean missing legal deadlines, such as notifying a data protection authority within 72 hours under GDPR.

14 · Compliance

Breaking this policy may lead to access being removed and to disciplinary action under [disciplinary policy]. IT may monitor the use of AI tools on company systems in line with [monitoring policy] and applicable law.

15 · Review

The Policy Owner reviews this policy every 6 months, and whenever we adopt a significant new AI tool, the law changes, or an incident shows it needs updating.

Acknowledgement

I have read and understood the [Company name] AI Acceptable Use Policy. I agree to follow it, and to ask [Policy Owner] if anything is unclear.

Name	_____	Role	_____
Signature	_____	Date	_____

Take the Next Step

Need help putting AI governance in place? Alphatechs helps businesses set up secure AI use, from policy and access controls to monitoring and staff training. Free 30-minute call: alphatechs.al/contact

Take the free **SME Cyber Readiness Checklist 2026**: alphatechs.al/cyber-month

Template provided free by Alphatechs for Cybersecurity Awareness Month 2026. You may adapt and use it within your organisation. Provided "as is" as general guidance, not legal advice.