

AI Policy Pack

A ready-to-use AI policy for your organisation — produced by We Do Your Group

About this pack

This pack gives you a complete, plain-English AI policy in a single document. It covers Acceptable Use (what staff can and cannot do with AI tools), External AI Tools (the rules around ChatGPT, Claude, and similar), and a Sensitivity Label Framework for Microsoft 365 and Copilot. All company-specific details have been replaced with placeholders so you can adapt it quickly.

What to customise

Replace each placeholder below, then update the branding to match your own identity.

Placeholder	Replace with
[COMPANY NAME]	Your full legal company name (e.g. IT Solutions Limited)
[COMPANY NUMBER]	Your Companies House registration number
[REGISTERED ADDRESS]	Your registered office address
[VERSION] and [DATE]	Version number (e.g. 1.0) and the date the policy takes effect
[REVIEW DATE]	When the policy should next be reviewed (we recommend 12 months)
Colours and fonts	Update heading colours, accent colours, and fonts to match your brand guidelines

Produced by We Do Your Group • 0117 911 8808 • support@wedoyour.group • wedoyour.group

We Do Your Group is a Bristol-based managed IT services provider. We help businesses use technology safely and effectively — including Microsoft Copilot and AI adoption. If you need help implementing this policy, configuring Microsoft 365 sensitivity labels, or rolling out Copilot, we're happy to help.

AI Policy Pack

Acceptable Use · Sensitivity Labels · Governance

[COMPANY NAME] | [VERSION] | [DATE]

About this document

This pack consolidates everything you need to know about using AI tools safely and effectively at [COMPANY NAME]. Rather than a separate document for every policy area, we have brought together the key guidance into one plain-English reference that is easy to follow day to day.

The pack covers three areas:

- Acceptable Use Policy — what you can and cannot do with AI tools, including Microsoft Copilot
- External AI Tools Position — our stance on tools like ChatGPT and Claude, and what data must never leave Microsoft 365
- Sensitivity Label Framework — the agreed labels we use across Microsoft 365 to support safe Copilot use

A note on governance

Given the size of the team, we have kept governance intentionally light. There is no separate governance framework document here — the ownership and decision-making is straightforward: if in doubt, ask. Day-to-day, the technical controls and the guidance in this pack are what matter most.

An Approved Use-Case Register will be created once the team has had some hands-on time with Copilot — the best use cases come from real experience, not speculation.

Section 1: AI Acceptable Use Policy

1.1 Purpose

This policy sets out clear, practical guidance on how every team member can and cannot use AI tools — including Microsoft Copilot and any other AI assistant — in the course of their work at [COMPANY NAME].

The goal is not to restrict what AI can do for you. It is to make sure we use it responsibly, protect client data, and stay on the right side of our legal and professional obligations.

1.2 Scope

This policy applies to all team members, contractors, and anyone accessing [COMPANY NAME] systems. It covers all AI tools — whether accessed through Microsoft 365 (Copilot), a web browser (ChatGPT, Claude, Gemini, etc.), or any other platform.

1.3 Microsoft Copilot — our primary AI tool

Microsoft Copilot (accessed through Microsoft 365) is our approved, primary AI assistant. It is the right tool for most day-to-day AI tasks because:

- Data stays within our Microsoft 365 tenant — it does not leave our environment
- It integrates with our emails, documents, Teams, and calendar
- It respects the sensitivity labels we apply to content (see Section 3)
- It is covered by our Microsoft licensing and data processing agreements

You are encouraged to use Copilot to help with writing, summarising, drafting emails, analysing data, creating content, and exploring ideas. The training platform included with your licence is the best place to start — you do not need to figure it out on your own.

1.4 What you can use AI for

The following uses are permitted and encouraged:

- Drafting, editing, and improving documents, emails, and proposals
- Summarising long documents, meeting notes, or email threads
- Researching topics, generating ideas, or brainstorming
- Creating templates, checklists, or structured content
- Analysing data, formatting spreadsheets, or building formulas
- Writing or explaining code and scripts for internal tooling
- Generating images or creative content for internal or approved external use
- Learning — asking AI to explain concepts, technologies, or processes

1.5 What you must not use AI for

The following are not permitted:

- Entering client personal data, confidential client information, or commercially sensitive data into any external AI tool (see Section 2)
- Submitting AI-generated content to clients as your own work without reviewing, editing, and taking ownership of it
- Using AI to make final decisions that should involve human judgement — particularly anything affecting clients, finances, or HR
- Bypassing or attempting to bypass any security controls, data classifications, or access restrictions
- Using AI to generate content that is misleading, discriminatory, or in breach of our values
- Using personal AI accounts or consumer-grade tools to process any company or client data

1.6 Your responsibilities

AI tools produce output that can be plausible but wrong. You are responsible for anything you send, submit, or publish — whether AI helped create it or not. Before using AI-generated content:

- Read it properly — do not just copy and paste
- Check facts, figures, and any technical detail
- Make sure the tone and accuracy reflect our standards
- Apply your professional judgement

Think of AI as a very fast, very capable colleague who occasionally makes things up. You would not send a colleague's draft without reading it first.

1.7 Data handling

The single most important rule: never enter client personal data, confidential client information, or anything marked Client Confidential or Highly Confidential (see Section 3) into any AI tool outside of Microsoft 365.

If the data could cause harm, embarrassment, or a breach of trust if it were made public, it does not go into an external AI tool. Full stop.

Within Microsoft 365 and Copilot, sensitivity labels control what Copilot can and cannot access. Apply the right label to your content and Copilot will respect it automatically.

1.8 Reporting concerns

If you are unsure whether a use of AI is appropriate, ask before proceeding. If you become aware of a potential data breach or misuse of AI tools, report it immediately in the same way you would any other security incident.

Section 2: External AI Tools — Position Statement

This section sets out our position on AI tools accessed outside of Microsoft 365, so there is no ambiguity about what is and is not acceptable.

2.1 Our position in plain English

Microsoft Copilot (within Microsoft 365) is our main AI assistant. It should be the first tool you reach for.

We recognise that other AI tools — such as ChatGPT, Claude, Google Gemini, Perplexity, and others — can be genuinely useful for certain tasks, particularly research, personal learning, or exploring ideas. We are not banning these tools. However, their use is subject to one firm rule:

No company data, client data, or anything you would not want shared publicly must ever be entered into an external AI tool. When in doubt, use Copilot instead.

2.2 When external tools are acceptable

You may use external AI tools (such as ChatGPT or Claude) for:

- Personal learning or professional development
- Research using only publicly available information
- Creative or exploratory tasks that involve no company or client data
- Generating draft content that you will then substantially rewrite and review before using

2.3 When external tools are not acceptable

You must not use external AI tools for any task that involves:

- Client names, contact details, or any personal data relating to clients or their employees
- Confidential client information — technical, commercial, or operational

- Internal financial information, pricing, contracts, or commercial terms
- Employee personal data or HR-related information
- System details, credentials, network information, or security configurations
- Anything labelled Client Confidential or Highly Confidential (see Section 3)

2.4 Key tools and their status

Tool	Status	Notes
Microsoft Copilot (M365)	Approved — primary tool	Data stays in our M365 tenant. Use for all work-related AI tasks.
ChatGPT (OpenAI)	Conditional use	No company or client data. Acceptable for research and personal learning only.
Claude (Anthropic)	Conditional use	No company or client data. Acceptable for research and personal learning only.
Google Gemini	Conditional use	No company or client data. Use with the same care as ChatGPT.
Other consumer AI tools	Conditional use	Apply the same rules. If unsure, ask.

Section 3: Sensitivity Label Framework

Sensitivity labels tell Microsoft 365 — and Copilot — how to handle your content. Applying the right label is one of the most important things you can do to make Copilot work safely.

Labels are applied in Microsoft 365 apps (Word, Excel, Outlook, Teams, etc.) and stay with the file wherever it goes. Copilot uses these labels to understand what it can and cannot reference in its responses.

3.1 Our four labels

Label	What it means and when to use it
 Public	Information that can be freely shared outside the business. Marketing content, published blog posts, public-facing materials. Copilot can use this content freely.

Label	What it means and when to use it
 Internal	General internal content that is not sensitive but not intended for external distribution. Day-to-day emails, internal guides, team updates. The default for most content. Copilot can use this content within our tenant.
 Client Confidential	Any content relating to a specific client – their data, their systems, their commercial arrangements. Must never leave Microsoft 365. Copilot can use this content but will not mix it into responses for other clients.
 Highly Confidential	The most sensitive content – HR records, financial data, credentials, legal matters, board-level information. Strictly controlled. Copilot access is restricted by default for this label.

3.2 How to apply a label

In most Microsoft 365 apps you will see a sensitivity bar or a Sensitivity button in the ribbon. Select the appropriate label before saving or sharing. If a file does not have a label, Microsoft 365 will ask you to apply one.

- New documents: apply a label when you create the file
- Emails: apply a label in Outlook before sending – especially for anything client-related
- Teams channels and SharePoint sites: labels can be applied at the site level by your administrator

If you are unsure which label to apply, default to Internal and check with your manager. It is always better to apply a more restrictive label and relax it later than to under-classify sensitive content.

3.3 Labels and Copilot

Copilot respects sensitivity labels automatically:

- Public and Internal content is accessible to Copilot in the normal way
- Client Confidential content is accessible to Copilot but isolated – Copilot will not surface one client's information in a response for another client
- Highly Confidential content has restricted Copilot access – this content will not be included in Copilot responses by default

This means the labels protect you. If you apply them correctly, Copilot cannot accidentally reference a client's confidential data in an unrelated task.

3.4 Quick reference

When in doubt: Internal is the safe default for most day-to-day content. Client Confidential for anything touching a client. Highly Confidential for anything you would only share on a strict need-to-know basis.

Document Information

Version	[VERSION]
Date	[DATE]
Owner	[COMPANY NAME]
Review date	[REVIEW DATE]
Classification	Internal

[COMPANY NAME] is a Limited company registered in England and Wales with registered number [COMPANY NUMBER] whose registered office is at [REGISTERED ADDRESS].