

Employee AI Use Policy

Replace every [bracketed] item before issuing. Version [number], dated [date], owned by [role].

1. Purpose and scope

[Company] permits the use of artificial intelligence tools where they help us do our work well, and sets rules so that their use does not expose our customers, our employees or the company to harm. This policy applies to all employees, contractors and temporary staff, on any device, when working for [Company]. It covers generative AI assistants, AI features built into software we already use, including [name the suites you license], and any tool that produces text, images, code, audio, summaries, scores or recommendations from a model. It applies whether the tool is paid for by the company or free.

2. Approved tools

The following tools are approved for work use, on the plan stated and under the company contract: [tool, plan, contract owner]. Tools not on this list, including free consumer versions of approved products and AI features switched on inside other software, are not approved for any company information above the public tier. To request a tool, contact [role or email]. Requests are answered within [number] working days. A tool is added only after [IT security or legal] has reviewed its data terms.

3. Information you may and may not enter

We classify information in three tiers. Public: information already published by the company or freely available. Internal: ordinary business information not intended for publication. Restricted: personal data about customers, employees or candidates; health information; payment card data; source code and credentials; unreleased financial results; information received under a non-disclosure agreement; and anything a lawyer has marked privileged.

You may enter public information into any approved tool. You may enter internal information only into approved tools on a business or enterprise plan whose terms exclude training on our data. You may not enter restricted information into any AI tool unless [legal or security] has approved that specific tool for that specific category in writing. Removing names does not make personal data public.

4. Confidentiality and privilege

Entering information into an AI tool is a disclosure to the tool's provider. Trade secrets lose protection if they are not kept secret, and legal privilege can be lost by disclosure to a third party. If you are unsure whether something is restricted, treat it as restricted and ask [role or email].

5. Accuracy and human review

You are responsible for everything you produce with an AI tool, as if you had written it yourself. AI output can be wrong, invented or out of date. Verify facts, figures, citations and code before you rely on them.

The following outputs must be reviewed and approved by the named role before use: anything published or sent to customers, regulators or the press ([role]); contracts and legal documents ([role]); code deployed to production ([role]); and any document that will be used in a decision about hiring, pay, promotion, discipline or dismissal ([role]).

6. Disclosure

Tell your manager or client when AI produced a substantial part of a deliverable, if they ask or if the engagement terms require it. Do not present AI output as independent research or as a human expert's opinion. Where the law requires notice to a candidate, employee or customer that an automated tool was used in a decision about them, [HR or legal] will provide that notice and you must not use the tool until they confirm it has been given.

7. Intellectual property and copyright

Do not ask a tool to reproduce copyrighted text, images, code or music, or to imitate an identified living person's voice or likeness. Do not enter third-party material we do not have the right to use. Treat AI output that we publish as potentially unprotected by copyright and raise it with [legal] if ownership matters, for example in product names or logos. Code generated by AI is subject to the same license review as any other code.

8. AI in employment decisions

No AI tool may be used to screen, rank, score, select, evaluate or make recommendations about candidates or employees, or to analyze their video, voice, writing style or online presence, unless the use has been approved in writing by [HR director and legal counsel]. Any approved use must have a named human decision-maker who reviews the primary evidence and can override the tool, must comply with the notice, audit and record-keeping duties of the jurisdictions where our candidates and employees are located, and must be recorded in the AI register kept by [role].

9. Monitoring and records

[Company] [does / does not] log the use of approved AI tools on company systems and accounts. Where we do, the log records [the tool used, the user, the time, and whether restricted information was detected], it is held for [number] days, it is accessed only by [named roles] and only for a security or compliance reason, and it is not used to measure individual productivity. Where state law requires a separate notice of electronic monitoring, it is attached to this policy. AI outputs used in a business record are kept for as long as that record is kept.

10. Vendors and third parties

Before a new AI tool or an AI feature of an existing vendor is approved, [role] confirms in writing whether the provider trains on our data, how long inputs and outputs are retained, where they are stored, who at the provider can read them, and whether the contract allows our security and legal teams to audit. Vendors who use AI to perform work for us are bound by the same data rules.

11. Security and incident reporting

Do not install browser extensions or desktop AI agents without IT approval. Do not give an AI agent credentials, payment methods or write access to company systems without [security] approval. If you believe restricted information has been entered into an unapproved tool, or an AI output has caused harm, report it to [security email] within [number] hours. Reporting in good faith will not be held against you.

12. Training, acknowledgment and review

All staff complete the AI use training within [number] days of hire and annually. This policy is owned by [role], reviewed every [number] months and whenever the law or our tool list changes. A breach of this policy is handled under the disciplinary procedure. Nothing in this policy limits your rights under federal or state law, including your right to discuss working conditions with colleagues.

Acknowledgment

I have read the [Company] AI Use Policy dated [date]. I understand which tools are approved, which information I may not enter, when a person must review the output, and who to ask.

Name: _____ Signature: _____ Date: _____

Template from WorkIntel Hub (workintelhub.com). Free to use and adapt. Not legal advice.