New Dynamics

AI at work

AI acceptable use: a workplace policy framework

Define approved AI use, information boundaries, human review and practical incident reporting.

Practical guidance · Worked examples · Printable worksheet

New Dynamics Editorial Team
Published 15 September 2026

www.new-dynamics.com
contact@new-dynamics.com

Inside this guide

Read in order for the full approach, or use the linked contents to find a section. The final worksheet gives you space to record decisions and next steps.

Define approved AI use, information boundaries, human review and practical incident reporting. This practical guide to AI acceptable use policy brings together a step-by-step approach, illustrative examples, a reusable worksheet and answers to common questions. Start with the section closest to your current challenge, then use the working session to turn the guidance into a clear next action.

Make the policy usable at the point of work

An AI acceptable-use policy should help employees decide which tool they can use, what information they can enter and what review is required. A general warning to “use AI responsibly” is not enough when someone is about to paste a confidential document into a service.

This framework needs adaptation to the organisation’s tools, contracts, data rules and local obligations. Define its scope, owner and effective date. Keep the approved-tool register somewhere employees can actually find it.

Draft clear permitted and restricted uses

A starting clause is: “Use only approved AI tools for approved work purposes. Follow the information restrictions for each tool. You remain responsible for checking outputs before using or sharing them.” Link that statement to the actual approval register and workflow.

Specify which information is excluded or requires separate authorisation. Include personal information, confidential commercial material and credentials. Do not imply that removing a name always makes a record anonymous. Context can identify a person or reveal sensitive work.

State which uses require specialist review or are prohibited by organisational policy. Consequential employment decisions, surveillance or attempts to infer sensitive personal characteristics need particular scrutiny. An acceptable-use policy is not a substitute for reviewing the legality and suitability of a proposed system.

Explain review and escalation

Describe how factual claims, calculations, citations and policy interpretations should be checked. A reviewer must have access to the source and enough knowledge to recognise an error. “A human clicks approve” is not a meaningful control if they cannot assess the output.

Provide an incident route for accidental disclosure, harmful output or unexpected behaviour. Tell people what to record and who will contain the issue. Encourage early reporting without asking employees to investigate a potential data incident themselves.

Worked example: rewriting a review note

Illustrative scenario: a manager wants help improving the wording of a performance note. The policy directs them to an approved tool and the applicable information boundary. If employee records are not approved for that tool, the manager uses a fictional example or writes the note manually.

Any permitted draft is checked against the original observation. The manager removes unsupported personality claims and remains responsible for the final content. A polished sentence does not become evidence of an event.

Policy completion checklist

- Publish approved tools, purposes and responsible owners.
- State permitted information and exclusions for each tool.
- Define prohibited uses and requests needing separate approval.
- Explain output review and accountability before sharing.
- Provide a simple incident and question route.
- Set training, acknowledgement and review arrangements.
- Test the policy with ordinary employee scenarios before adoption.

Keep the policy aligned with reality

Review tool changes, supplier terms and new use cases through a named process. Remove access when approval ends and explain alternatives. Ask employees where the policy is unclear or where workarounds are emerging.

Use the AI literacy guide to turn the rules into practice. Consult the NIST AI RMF Playbook as a general risk-management reference while adapting controls to your organisation.

Put the guide into practice

Set aside a working session with the people who own this process and one or two people who experience it. Use a fictional or appropriately authorised case, so the discussion can be specific without sharing unnecessary personal information. The purpose is to leave with a usable decision or document, not just agreement that the topic matters.

Prepare the case

Collect common employee questions about approved tools, information and output sharing. Use fictional examples from actual work categories. Identify where existing security or privacy rules already provide an answer and where an AI-specific instruction is needed. Avoid creating a second policy that contradicts the organisation’s established information controls.

Write the starting assumptions down before discussing solutions. If the group disagrees on what happened, identify the information needed to resolve that difference rather than building a plan on an untested story.

Work through the decision

Apply the draft policy to a routine drafting task and a task involving employee records. Ask participants to find the approved route and explain the required review. If they cannot identify whether a tool or data type is permitted, improve the register or wording before requiring acknowledgement.

Ask each participant to explain the proposed decision in their own words. Differences in interpretation often reveal an unclear criterion, a missing responsibility or an instruction that will be difficult to follow.

Test an exception

Test an accidental paste into the wrong tool, an embedded AI feature enabled by a supplier and a request from a senior colleague to skip review. Identify the reporting or approval route for each. The policy should remain usable under pressure and should not depend on an employee challenging a manager without support.

Record what changes in this situation and what remains the same. An exception should lead to a clear next step, with an owner, rather than an informal workaround that nobody can explain later.

Agree the handoff

Give employees a short decision aid linked to the full policy and tool register. Confirm who maintains it and how changes are communicated. Managers need a route to request a new use case, while service owners need authority to suspend a tool when a material issue is discovered.

Finish by confirming the owner, the next action and the date when the result will be reviewed. Give the person receiving the work enough context to continue without repeating the whole discussion.

Frequently asked questions

Should we ban all AI tools at work?

That is an organisational decision based on risks, needs and available controls. A blanket rule can be difficult to apply when AI features are embedded in ordinary software. Map actual uses and provide clear approved routes where appropriate. If a use is restricted, explain the boundary and alternative workflow so employees can complete their work without guessing or creating hidden workarounds.

Can employees use personal AI accounts for company work?

Only if the organisation’s policy and reviewed arrangements permit the specific use and information. Personal accounts may have different terms, controls and administration from an approved workplace service. Do not assume that paying for an account makes it suitable. State the rule clearly and provide a route for questions before employees enter confidential or personal information.

What should employees do after an accidental disclosure?

Use the organisation’s incident route promptly and preserve the information needed for an authorised response. The policy should explain the contact and the relevant facts to report without requiring the employee to investigate alone. Avoid making promises about deletion or notification before the responsible team assesses the situation. Early reporting supports containment and a more informed response.

Review the first cycle

Review whether employees can apply the policy to realistic tasks and whether the approved-tool register stays current. Examine questions and reported errors for unclear boundaries. Update training when the policy changes, and check that managers follow the same rules they expect employees to use.

Keep a brief record of what was tried, what participants found useful and what needs to change. Compare the result with the original problem rather than judging success only by completion. If the process created extra work without improving clarity, quality or support, simplify it and test again. Share the agreed change with the people who will use it, and name the person responsible for keeping the guidance current.

About New Dynamics

New Dynamics connects goals, feedback, recognition and reviews around the way organisations work. This guide is published by the New Dynamics Editorial Team as part of our practical library for HR leaders, managers and People teams.

Use the examples and worksheets to structure your own discussions and adapt them to your organisation. Illustrative scenarios are not customer case studies. Policy and employment guidance needs appropriate local review before adoption.

For questions about this guide, corrections or a conversation about your performance management process, email contact@new-dynamics.com. Explore the complete guide library for related resources.

Your working worksheet

Use the prompts from this guide to prepare one real conversation or decision. Keep personal or sensitive information in your organisation’s approved records. This page is for your own working notes.

Publish approved tools, purposes and responsible owners.

State permitted information and exclusions for each tool.

Define prohibited uses and requests needing separate approval.

Explain output review and accountability before sharing.

Provide a simple incident and question route.

Set training, acknowledgement and review arrangements.

Test the policy with ordinary employee scenarios before adoption.

Discuss your next step with New Dynamics: contact@new-dynamics.com