

AI Acceptable-Use Policy

The Operator's Manual for Artificial Intelligence

Template Kit — Document 1 of 6

IMPORTANT — BEFORE YOU USE THESE TEMPLATES

These templates are starting points for organizations without existing AI governance. They are not legal documents and are not a substitute for qualified legal counsel. Review and adapt them to your specific jurisdiction, industry, and situation before use. Do not implement any policy, form, or checklist from this kit without professional review. The Operator's Manual for Artificial Intelligence makes no representations as to their completeness, accuracy, or fitness for any particular purpose.

1. Document Information

Field	Entry
Organization Name	[Enter organization name]
Policy Title	AI Acceptable-Use Policy
Version	1.0
Effective Date	[Enter date]
Policy Owner	[Name and title]
Approved By	[Name and title]
Next Review Date	[Enter date — recommended annually]

2. Purpose

This policy establishes the rules for using artificial intelligence tools within [Organization Name]. It defines which tools may be used, by whom, and under what conditions. It protects the organization, its employees, its clients, and the people whose data may be involved.

This policy applies to all AI tools — including chat assistants, writing tools, code generators, image generators, and AI-enabled features within existing software — used in connection with any organizational task.

3. Scope

This policy applies to all employees, contractors, consultants, and third parties who use AI tools in connection with work for [Organization Name], regardless of whether they are using organizational devices or personal devices.

4. Approved AI Tools

Only the tools listed below are approved for use. Using AI tools not on this list for organizational work requires prior written approval from the Policy Owner.

Tool	Approved For	Who May Use	Restrictions
[Tool name]	[Describe permitted use]	[Role or team]	[Any limits]
[Tool name]	[Describe permitted use]	[Role or team]	[Any limits]
[Tool name]	[Describe permitted use]	[Role or team]	[Any limits]

5. Permitted Uses

AI tools may be used for the following purposes, subject to the risk controls in Section 7:

Permitted Use	Risk Level	Control Required
Drafting and editing documents	Low–Medium	Review before sending
Summarizing internal documents	Low–Medium	Review for omissions
Brainstorming and ideation	Low	Standard judgment
Rewriting or reformatting content	Low	Standard judgment
Generating code for internal review	Medium	Technical review before use
Research and background information	Medium	Verify against primary sources

6. Prohibited Uses

The following uses are prohibited. This list is not exhaustive. When in doubt, treat the task as prohibited until the Policy Owner confirms otherwise.

Prohibited Action	Why	Risk Level
Pasting personally identifiable information (PII)	Data exposure; may breach privacy law	Prohibited Without Governance
Pasting credentials, passwords, or API keys	Immediate security risk	Prohibited Without Governance
Pasting confidential client or patient data	Regulatory and legal exposure	Prohibited Without Governance
Pasting non-public financial data or trade secrets	Competitive and legal exposure	Prohibited Without Governance
Using AI output for legal, medical, or financial decisions without expert review	High error risk; professional liability	Critical
Allowing AI to take automated actions without human approval	Irreversible system actions; lack of oversight	Critical / Prohibited
Presenting AI-generated content as your own work without disclosure (where required)	Integrity and regulatory risk	High

Prohibited Action	Why	Risk Level
Using unapproved AI tools for organizational work	Unknown data handling; no governance	Prohibited Without Governance

7. Review Requirements by Risk Level

Use the Risk Ladder from The Operator's Manual for Artificial Intelligence to determine the required level of review before acting on any AI output.

Risk Level	Required Action Before Use
Low	Apply standard judgment. No additional review required.
Medium	Review output before sending to others or using in a decision.
High	Verify against a primary source or qualified expert. Document the verification.
Critical	No action without formal human approval. Log the decision. No autonomous action.
Prohibited Without Governance	Do not proceed. Escalate to Policy Owner for review before taking any action.

8. Accountability

Policy Owner: The individual named in Section 1 is responsible for maintaining this policy, reviewing incidents, and approving exceptions.

All Users: Employees and contractors are responsible for reading this policy, applying it to their daily work, and reporting incidents or concerns promptly.

Managers: Managers are responsible for ensuring their teams understand and follow this policy.

9. Incident Reporting

Report any suspected AI-related incident — including accidental data exposure, unsafe outputs, unexpected automated actions, or policy violations — immediately to:

Contact	Details
Policy Owner	[Name, email, phone]
IT Security	[Contact details]
Legal / Compliance	[Contact details]

Complete an AI Incident Log (Template 4 of this kit) for any confirmed incident. Retain the log for a minimum of [enter period, e.g., 2 years].

10. Compliance and Consequences

Violation of this policy may result in disciplinary action up to and including termination, legal action, or reporting to relevant regulatory authorities depending on the nature and severity of the violation.

11. Review Schedule

This policy must be reviewed at least annually or whenever a significant change occurs — such as the adoption of a new AI tool, a regulatory change, or a significant incident.

12. Acknowledgment

By signing below, I confirm that I have read, understood, and agree to comply with this Acceptable-Use Policy.

Full Name	Job Title / Role
Signature	Date
Team / Department	Employee ID (if applicable)