AI Acceptable Use Policy

Template for Ontario businesses. Replace everything in [square brackets], delete what does not apply, and have it reviewed by your own legal counsel before you adopt it.

Free template from IT Rapid Support Inc., itrapidsupport.com. Legal references checked November 10, 2026. This template is general information, not legal advice.

Policy owner	Approved by	Effective date	Version	Next review
[Name, role]	[Name, role]	[Date]	[1.0]	[Date, at most 12 months out]

1. Purpose

[Company name] allows staff to use artificial intelligence (AI) tools where they help us work better, and only in ways that protect our clients, our employees and our information. This policy sets out which AI tools are approved, what information may and may not go into them, who is responsible for what they produce, and when we tell people that AI was used.

2. Who and what this policy covers

- Everyone who works for or with [Company name]: employees, contractors, temporary staff and volunteers.
- Any AI tool used for work, on a company device or a personal one: chat assistants, writing and image tools, meeting note-takers, AI features built into software we already use, browser extensions and plugins.
- Any work information, including client, customer and employee information, whatever form it is in.

3. Approved AI tools

Only the tools in this table may be used for work. Use them only through the company account listed, never a personal account. Anything not listed is not approved until [policy owner] adds it.

Tool	Account to use	Approved for	Highest information class allowed (section 5)
[Tool name]	[Company tenant / licence]	[e.g. drafting, summarizing internal documents]	[Internal]
[Tool name]	[Company tenant / licence]	[ ]	[ ]
[Tool name]	[Company tenant / licence]	[ ]	[ ]

To request a new tool, send [policy owner] the tool name, what you want to use it for and what information it would touch. Before approval, we check where the data is stored, whether the vendor uses it to train its models, how long it is kept, and what admin and logging controls exist.

4. Prohibited uses

- Using a personal or free account of any AI tool for work.
- Entering information above the class allowed for that tool (section 5).
- Letting an AI tool make a final decision about a person (hiring, firing, discipline, pay, credit or service eligibility) without a human review.
- Using AI to create content that impersonates a real person, or that is misleading, discriminatory or harassing.
- Installing AI browser extensions, plugins or meeting note-takers that have not been approved.
- Connecting an AI tool to company email, files or calendars, or granting it access through a "sign in with" prompt, without IT approval.
- Uploading third-party material that we do not have the right to use.

5. Information rules

Use the lowest class of information that gets the job done. Where you can, remove names and other identifiers before you enter text into an AI tool.

Class	Examples	Allowed in AI tools?
Public	Published website content, press releases, public filings	Yes, in any approved tool
Internal	Internal procedures, non-sensitive drafts, general emails	Only in tools approved for Internal
Confidential	Client files, contracts, financial records, personal information about clients or staff	Only in tools approved for Confidential, and only where your role requires it
Restricted	Passwords and keys, health information, SIN and government ID numbers, banking details, legal advice, anything under a confidentiality order	Never

Personal information stays subject to Canadian privacy law when it goes into an AI tool. If personal information is entered into a tool that is not approved for it, report it to [privacy officer] immediately (section 10).

6. Human review and accountability

- A person reviews every AI output before it is used, sent or relied on, and is responsible for it as if they wrote it.
- Check facts, figures, names, citations and legal or technical statements against a reliable source. AI tools can produce answers that are wrong, incomplete or biased.
- Decisions remain the responsibility of [Company name] and the person making them, not of the tool.

7. Telling clients and others

Tell a client when AI has materially shaped work delivered to them, or when their contract or professional rules require it. [Add any client commitments or professional regulator rules that apply to your business.]

8. Hiring and HR

- If [Company name] has 25 or more employees on the day a job is posted, and AI is used to screen, assess or select applicants, the public job posting must say so (Ontario Employment Standards Act, 2000, s. 8.4, in force for postings from January 1, 2026). This applies even when a job board or recruiter posts the job for us.
- Any AI used in hiring, promotion, discipline or termination is checked for bias, and a person makes the final decision. The Ontario Human Rights Code protects against discrimination in employment.
- [If you have customers or employees in Quebec: if a decision about a person is based exclusively on automated processing of their personal information, tell them, explain on request what information and main factors were used, and let them ask a staff member to review it (Quebec private-sector privacy act, s. 12.1).]

9. Monitoring of AI use

[Company name] [does / does not] monitor how staff use AI tools on company systems. [If it does: describe how and in what circumstances, and what the information may be used for.] If we have 25 or more employees on January 1 of a year, this monitoring is also described in our written electronic monitoring policy under the Employment Standards Act, 2000.

10. Security and incidents

- Sign in to approved AI tools with your company account and multi-factor authentication.
- Do not keep prompts or outputs that contain personal information longer than the work needs, and do not reuse them for another purpose.
- Report immediately to [privacy officer / IT contact] if personal or confidential information went into a tool it should not have, if an AI tool behaves unexpectedly, or if you see a suspicious AI-generated message, call or video (for example, a request to move money).
- A privacy incident involving an AI tool is handled under our breach response procedure, including assessing whether it must be reported to the Privacy Commissioner of Canada.

11. Training, exceptions and review

- Everyone covered by this policy completes AI training when they join and [every year].
- Exceptions must be approved in writing by [policy owner], with a reason and an end date.
- Breaking this policy may lead to loss of access to AI tools and to discipline under our usual procedures.
- [Policy owner] reviews this policy at least every [12] months, and sooner if the law or our tools change.

12. Acknowledgement

I have read and understood this AI Acceptable Use Policy and agree to follow it.

Name	Role	Signature	Date

Appendix: the law and guidance behind this template

Checked November 10, 2026. Laws change; confirm the current position with your legal counsel.

Source	What it means for this policy	Where to read it
PIPEDA (federal private-sector privacy law)	Applies to personal information Ontario businesses handle in commercial activity; Ontario has no private-sector privacy law of its own. Breaches that create a real risk of significant harm must be reported to the Privacy Commissioner of Canada and the people affected told as soon as feasible, and every breach must be recorded.	laws-lois.justice.gc.ca/eng/acts/P-8.6/
Ontario Employment Standards Act, 2000, s. 8.4 and O. Reg. 476/24	Employers with 25 or more employees must disclose AI use to screen, assess or select applicants in publicly advertised job postings, for postings from January 1, 2026.	ontario.ca/laws/statute/00e41 ; ontario.ca/laws/regulation/r24476
Ontario Employment Standards Act, 2000, Part XI.1	Employers with 25 or more employees on January 1 must have a written electronic monitoring policy before March 1 of that year.	ontario.ca/laws/statute/00e41
Ontario Human Rights Code	Protects against discrimination in employment and other social areas.	ohrc.on.ca
OPC and provincial privacy regulators, Principles for responsible, trustworthy and privacy-protective generative AI technologies (December 7, 2023)	Use de-identified information in prompts where possible, enter personal information only where authorized, do not keep prompts unless required, and accountability stays with the organization.	priv.gc.ca (artificial intelligence guidance)
Canadian Centre for Cyber Security, Generative artificial intelligence (ITSAP.00.041)	Warns that staff may paste sensitive data into prompts and that outputs can be wrong or biased; recommends a usage policy with oversight and review.	cyber.gc.ca
Quebec private-sector privacy act, s. 12.1 (Law 25)	Notice and review rights when a decision is based exclusively on automated processing of personal	legisquebec.gouv.qc.ca (P-39.1)

	information.	
Ontario Enhancing Digital Security and Trust Act, 2024 (Bill 194)	Its AI rules apply to prescribed public sector entities, not private businesses. Relevant if you supply AI-enabled services to an Ontario public body.	ontario.ca/laws/statute/24e24
Federal AI legislation	The proposed Artificial Intelligence and Data Act (Bill C-27) died when Parliament was prorogued in January 2025. Bill C-36, the proposed Protecting Privacy and Consumer Data Act, was introduced June 15, 2026 and is not law.	parl.ca/legisinfo