PROTECT YOUR PRIVACY WHEN USING AI TOOLS

As AI becomes part of everyday life, these simple steps can help you safeguard your personal information when using these tools.

THINK BEFORE YOU SHARE

Information entered into an AI tool may be retained for long periods and be hard, or impossible, to delete. It can also be used in ways you didn't intend, including for training or to identify you or predict your behaviour.

Recommendations

- Only share what you'd be comfortable making public
- Avoid sharing passwords, financial details, identifying information, private conversations or confidential work data
- Use general descriptions instead of specifics

WATCH FOR INACCURACIES AND HALLUCINATIONS

AI can generate information that is incorrect, misleading, or invented, including fabricated facts, incorrect details, fake citations or overgeneralizations.

Recommendations

- Always verify responses, even when they sound convincing
- If your organization is using AI to make important decisions about people, make sure a human is involved in that process

PUT PRIVACY FIRST

Not all AI tools offer the same level of privacy protection. All tools must be transparent about why they're collecting, using or disclosing your personal information.

Recommendations

- Check out the tool's privacy settings and data retention policies
- Turn off training or personalization settings where possible, or avoid creating an account if not necessary to use the tool
- Delete past conversations regularly
- Disable AI app location access or microphone/camera access

KNOW YOUR RIGHTS

AI tools must comply with applicable privacy laws, including BC's *Personal Information Protection Act*. PIPA empowers you with rights when AI companies handle your personal information.

Recommendations

- You can request access to your personal information and ask for corrections
- If you believe your privacy rights have been violated, you have the right to complain to the OIPC

oipc OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA