KIRKE CONSULTING

Empowering transformation through expertise

AI & Automated Decision Readiness Checklist

A guide to responsible AI use, data protection and Bill C-36 preparedness.

*Prepared with reference to Bill C-36 (first reading June 15, 2026). This checklist is for general readiness purposes and is not legal advice.

Introduction

AI is already being used by organizations through productivity tools, analytics and vendor features, among others. Bill C-36 is not a general AI law, but it will create important privacy obligations where AI and other automated systems use personal information, particularly when they influence significant decisions about individuals.

Know Where AI Is Being Used

- ☐ We maintain an inventory of AI and automated systems that collect, infer, generate or use personal information.
- ☐ We know which systems use personal information, behavioural data, images, audio, biometrics or other sensitive information.
- ☐ New AI tools cannot be introduced solely through individual employees or vendor decisions without an appropriate review.
- ☐ Each material AI use case has a named business owner.

Governance and AI Vendors

- ☐ Procurement reviews AI-enabled vendors for privacy, security, data use, retention, model-training practices and sub-processors before approval.
- ☐ Contracts clearly restrict the vendor's use of the organization's data and require appropriate safeguards.
- ☐ We understand whether the vendor relies on third-party foundation models or other external AI services.
- ☐ We have documented requirements for breach notification, deletion, data return, service termination and changes to AI functionality.
- ☐ Material vendor changes to data use or AI functionality trigger a new review.

Protect Personal and Organizational Data

- ☐ Employees know what personal, confidential or proprietary information must not be entered into public or unapproved AI tools.
- ☐ We understand whether AI vendors use our prompts, files, proprietary documents or other submitted data to train or improve their models.
- ☐ We know where AI-related data is stored, who can access it, how long it is retained and whether it is transferred outside Canada.
- ☐ We minimize the personal information used by AI tools and avoid using sensitive information where the purpose can be achieved another way.
- ☐ Children's information receives a higher level of scrutiny because of its sensitivity.
- ☐ We can delete or retrieve information from AI-enabled systems when required by our policies, contracts or applicable law.

CONTACT US

KIRKE CONSULTING

Empowering transformation through expertise

Review Significant Automated Decisions

This is the area where Bill C-36 most directly intersects with AI governance.

- ☐ We distinguish low-risk productivity uses from uses that make or materially influence a prediction, recommendation or decision that could have a significant effect on an individual.
- ☐ We document the purpose of the system, the decision it supports and the role of human judgement in the final outcome.
- ☐ We know what personal information the system uses, the source of that information and the key factors that influence the output.
- ☐ We can provide a plain-language explanation of a significant automated outcome when required.
- ☐ A qualified employee can review the outcome and consider information or representations from the affected individual.
- ☐ We do not treat an AI-generated score, recommendation or flag as inherently accurate or objective.

Test Accuracy, Bias, and Data Quality

- ☐ The data used by AI-enabled systems is sufficiently accurate, complete and current for the intended purpose.
- ☐ We test important systems for false positives, false negatives, inconsistent outcomes and inappropriate bias before relying on them.
- ☐ We understand the limitations of AI-generated content and require verification when outputs may affect students or institutional decisions.
- ☐ We have a clear process for correcting inaccurate personal information or erroneous AI outputs.
- ☐ We monitor performance after implementation rather than assuming a vendor's pre-launch testing is sufficient.

Set Clear Rules for Employees

- ☐ Our acceptable-use policy explains when generative AI may and may not be used for business work and/or administrative activities.
- ☐ Employees understand when human review is mandatory and when AI should not be used to make or recommend decisions.
- ☐ Employees know how to report an AI-related privacy, security, accuracy or fairness concern.
- ☐ Training is refreshed as tools, school practices and legal requirements evolve.

Build AI Into the Existing Privacy Program

- ☐ AI is included in privacy impact assessments, technology reviews and vendor due diligence rather than managed as a separate one-time initiative.
- ☐ Privacy notices and internal policies accurately reflect material AI and automated decision uses.
- ☐ We retain enough documentation to explain why a tool was approved, what risks were identified and what controls were put in place.
- ☐ Leadership receives a periodic view of material AI use cases, incidents, exceptions and unresolved risks.
- ☐ We have a process to retire AI uses that no longer deliver sufficient value or cannot be operated within acceptable privacy and governance boundaries.