

When AI goes wrong

Keep this where the AI lead and managers can find it fast.
Being fast and honest matters more than being perfect.



Do these 4 things

1. **Stop.** Pause the tool or automation. Don't delete anything. Don't fix it alone.
2. **Tell the AI lead the same day.** [name] · [phone] · [email]
3. **Tell the people affected** as soon as you can. [number] days is the latest, not a reason to wait. Use the notice on the back.
4. **Fix it and learn.** Change what caused it. Write it in the incident log. Keep the log for 24 months.

What counts as a problem

- AI output went out with wrong facts, to the wrong person, or in the wrong tone.
- Personal information went into a tool it shouldn't have.
- An automation did something it wasn't allowed to do.
- Someone was fooled by a fake message, voice or image.
- A fake of one of our people was used on donors or clients. Also call the Canadian Anti-Fraud Centre: 1-888-495-8501.

Turn over for the notice to send to people affected.

Notice to people affected

Dear [name] ,

On [date] , we found that [what happened, in one or two plain sentences] .
This involved [what information or message] .

We have [what you did to stop it] . We are also [what you are changing so it does not happen again] .

We are sorry. If you have questions, please contact [name] at [phone or email] .

[Your name, role, organization]

For the AI lead: does the law say we must report it?

Check whether privacy law says you must report the breach, and to whom. The federal Privacy Commissioner's "real risk of significant harm" tool helps you decide.

Keep a record of every privacy breach for at least 24 months, even small ones.