



Privacy Breach Response

5 Step Action Plan

Step 1

Recognize a privacy breach, which can be spotted by anyone! A student, employee, administrator, client, volunteer, parent, automated alarm suspects or identifies a breach, tell your appointed Privacy Officer or notify the Privacy Commissioner right away.

CONTAIN THE BREACH

SPOT AND STOP

Step 2

Once identified as a privacy breach, an internal investigation is conducted by the Privacy Officer and team. *The team considers- was the breach accidental or intentional? What were the circumstances leading up? Will the incident happen again? What measures need be in place to avoid a future similar incident?*

INVESTIGATE THE BREACH

FORMAL OR INFORMAL

Step 3

Assess the risks associated with the breach in order to provide a response. *What data elements have been breached? What is the possible use for this information? What is the root cause? How many individuals are affected? Could any further harm result to the public?*

IMPACT/RISK EVALUATION

WHAT'S THE DAMAGE?

Step 4

Which legislation (policy or contract) applies and whether notification is mandatory or voluntary. (FOIP/PIPA/HIA) Review the risk assessment and notify if required or better yet, volunteered. Document your analysis and final decisions.

NOTIFICATION -WHO, WHEN, AND HOW

IS IT REQUIRED?

Step 5

Take the time to thoroughly investigate the cause of the breach once the risks associated with it have been mitigated, which should ultimately result in a plan to avoid future similar breaches of privacy.

PREVENTION

LEARN FROM MISTAKES