DURHAM CATHOLIC DISTRICT SCHOOL BOARD
Learning and Living in Faith

ADMINISTRATIVE PROCEDURE – AP201-2

Privacy Breach Protocol

Area: Governance
Policy Reference: Freedom of Information and Protection of Privacy (PO201)

Approved: October 3, 2016
Revised: June 17, 2025

1. Purpose

The Durham Catholic District School Board (the "Board") recognizes that when personal information is collected, used, retained and/or disclosed while meeting its statutory duties and responsibilities, it should be managed in a manner that respects the privacy of the individual in keeping with the parameters of this policy. This procedure applies to all employees and service providers associated with the Board.

The purpose of this administrative procedure is to establish a framework for responding to privacy breaches within the Board, ensuring compliance with Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024, and other relevant legislation.

2. Definitions

Personal Information (*as defined by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*) – is recorded information about an identifiable individual which shall be treated as confidential unless it is public information or, unless the individual consents to its disclosure or, disclosure of the information is otherwise permitted by MFIPPA.

3. Procedures

3.1 A privacy breach occurs when personal information is accessed, disclosed, or used without authorization. This includes incidents such as theft, loss, cyber-attacks, or inadvertent disclosures. The following actions must be taken upon learning of a privacy breach:

3.1.1 Any employee or volunteer who identifies or suspects a privacy breach must report it immediately to their supervisor, who will verify the breach with the

supervising member of senior administration and contact the Chief Information Officer – Freedom of Information and Privacy, if necessary;

3.1.2 The Chief Information Officer – Freedom of Information and Privacy will document the breach details, including time, nature, and scope, and if necessary, initiate the Cyber Incident Response Plan (CIRP) to detect, respond to, recover from, and prevent future incidents;

3.1.3 The reporting individual will be asked to provide details of the potential breach;

3.1.4 The Information and Communications Technology department (ICT) will conduct a privacy impact assessment (PIA) as mandated by Bill 194 to evaluate the breach's extent and impact, considering factors such as:

a) The sensitivity of the information;

b) The number of individuals affected; and

c) Potential harm (e.g., identity theft, reputational damage).

3.1.5 If it is determined that a breach has occurred, the reporting individual will be asked by ICT to do the following, in consultation with the appropriate staff:

a) Take immediate steps to contain the breach, such as securing affected systems, retrieving hard copies of any personal information that has been disclosed, or suspending compromised accounts. ICT will provide technical support in containment efforts;

b) Attempt to ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information;

c) Determine whether the breach would allow unauthorized access to any personal information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system);

d) Notify individuals whose privacy was breached, by telephone or in writing, providing:

- A description of the breach;
- Potential impacts;
- Steps being taken to address it;
- If necessary, advise on protecting themselves (e.g., monitoring accounts); and
- Where appropriate, provide contact information for the IPC.

3.1.6 ICT will contact the Information Privacy Commissioner (IPC), if necessary, to ensure that all legislative obligations are fulfilled;

3.1.7 Detailed records of the breach and response actions taken will be maintained centrally; and

3.1.8 ICT will conduct an investigation to identify the root cause of the breach and implement corrective measures, such as updated security protocols or staff training, to prevent recurrence.

4. Sources

4.1 Freedom of Information and Protection of Privacy Act (FIPPA)
4.2 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
4.3 Personal Health Information Protection Act (PHIPA)
4.4 Information and Privacy Commissioner-Ontario (IPC) Privacy Breach Protocol Guidelines for Government Organizations
4.5 Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024

5. Appendices

Nil

6. Related Policies and Administrative Procedures

6.1 Freedom of Information and Protection of Individual Privacy Policy (PO201)