ANGLOPHONE WEST SCHOOL DISTRICT

POLICY NO. ASD-W-801-1A

PRIVACY BREACH PROTOCOL – APPENDIX A

Category:	Data, IT and Records Management	**Effective:**	September 2022

Introduction:

The Anglophone West School District (ASD-W) is committed to collecting, using, disclosing and disposing of personal information entrusted to it in a manner that is accurate, confidential, secure and private.

ASD-W has created this Privacy Breach Protocol to follow should a privacy breach occur within the District.

What is a Privacy Breach?

As per the *Right to Information and Protection of Privacy Act* (the RTIPPA) and the *Personal Health Information Privacy and Access Act* (the PHIPAA), ASD-W must investigate and respond to any suspected or actual privacy breaches that occur within the District.

A privacy breach means any incident of unauthorized access, use, disclosure or disposal of personal information in the custody of or under the control of a public body. Privacy breaches can occur in a number of ways. Some of the more common incidents include:

- Loss or theft of mobile devices (e.g. laptops, USB sticks)
- Misdirected communications (via email, fax or mail)
- Employee "snooping" (also known as unauthorized access to or misuse of information by an employee)
- Hacking of computers, servers and websites
- Malicious software ("malware") attacks, including ransomware
- Phishing or social engineering attacks
- Stolen paper records from an employee's vehicle, home or office
- Improper disposal of records or devices

ASD-W Breach Protocol:

1. **BREACH REPORTED**: When an actual or suspected privacy breach occurs, the employee responsible for or who discovers the breach must notify their supervising District or School Administrator to whom they report directly. Additionally, the supervising District or School Administrator is responsible for informing the ASD-W RTIPPA Coordinator of the breach.

2. **BREACH CONTAINED**: The RTIPPA Coordinator, in consultation with the District or School Administrator, involved, the employee responsible for or who discovers the breach, and other relevant staff, will take immediate steps to contain the breach.
3. **INDIVIDUALS NOTIFIED**: The District or School Administrator, in consultation with the RTIPPA Coordinator, shall notify all affected individuals.
4. **BREACH DOCUMENTED**: The District or School Administrator will fill out the Privacy Breach Incident Report **(See Appendix B)** in consultation with the employee(s) involved and other relevant staff as necessary.
5. **BREACH EVALUATED**: The Privacy Breach Incident Report will document a summary of the assessment and findings. The RTIPPA Coordinator will evaluate the breach, considering the potential harm (risk) to the affected individual(s). Depending on the severity of the breach, the RTIPPA Coordinator will notify the Ombud's Office, as required by privacy legislation (i.e., if the breach falls under the definition of significant harm or if the breach involved personal health information.)
6. **IDENTIFYING CORRECTIVE MEASURES**: As part of the Privacy Breach Incident Report, corrective measures will be recommended to prevent future breaches.
7. **CLOSING THE FILE**: Once the breach has been evaluated, the RTIPPA Coordinator will submit the final Privacy Breach Report to the superintendent and district or school administrator involved. Depending on the severity of the breach, the report may also be sent to the other senior administrators. The breach will be logged in the Privacy Breach Incident Log.

Roles and Responsibilities:

Note: Some steps may happen simultaneously.

	Step	Description	Responsibility
1	Reporting the Breach	Staff must immediately notify their supervising District or School Administrator of the breach. In addition, the supervising District or School Administrator must inform the RTIPPA Coordinator.	ASD-W Staff, Supervising District or School Administrator
2	Containing the Breach	The RTIPPA Coordinator, in consultation with the supervising District or School Administrator, the employee responsible for or who discovers the breach, and other relevant staff, will determine how to contain and mitigate the breach appropriately.	RTIPPA Coordinator, Supervising District or School Administrator, ASD-W Staff

		Depending on how the breach occurred and the severity of the breach, different steps for mitigation can be taken, which can include: ○ Stopping the unauthorized practices; ○ Recovering the records and all copies; ○ Shutting down the system that was breached; ○ Revoking or changing computer access codes; and ○ Correcting the weakness in physical and/or electronic security.	
3	Notifying Affected Individuals and Others	AFFECTED INDIVIDUAL(S) Notification should occur as soon as possible following a breach. The preferred method is direct notification: by phone, letter, email, or in person. Indirect notification via the website or public notice generally only occurs when direct notification could cause further harm, is prohibitive in cost or lacks contact information for the affected individuals. Using multiple notification methods in some instances may be the most effective approach. Considerations Favouring Direct Notification • The identities of individuals are known • Current contact information for the affected individuals is available • Individuals affected by the breach require detailed information to protect themselves from harm arising from the breach properly • Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.) Considerations Favouring Indirect Notification • A very large number of individuals are affected by the breach, such that direct notification could be impractical • Direct notification could compound the harm resulting from the breach	RTIPPA Coordinator, Supervising District or School Administrator, ASD-W Staff

		The RTIPPA Coordinator determines the scope of the notification in consultation with the supervising District or School Administrator and other relevant staff. The following will be considered: a) The mechanism for notification (direct mail/email and/or phone, public notice, media, website, etc.); b) What should be included in the notification; c) When should the notification occur; and d) Who should notify the affected individuals? Upon notification, concerns raised by the individual should be addressed as fully as possible, including, within reason, exploring additional corrective measures and suggesting they also have the option to contact the Ombud's office. In some circumstances, direct notification of the affected individual is not possible or is not recommended. In this case, a substitute decision-maker will be notified on behalf of the affected individual. For example, if a child is under 16, a notification will be sent to the parent or legal guardian. DISTRICT STAFF Depending on the nature or seriousness of the breach, the RTIPPA Coordinator will determine the additional staff to be notified, including whether or not the situation merits advising other Senior Administrators, or the Superintendent. POLICE If the breach appears to involve theft or other criminal activity, the RTIPPA Coordinator, in consultation with the supervising District or School Administrator, will immediately contact the police and notify other relevant staff of the notification.	

		OMBUD (Provincial Privacy Office) Depending on the severity of the breach, the RTIPPA Coordinator will notify the Ombud's Office of the breach, as required by privacy legislation (i.e., if the breach falls under the definition of significant harm or if the breach involved PHI). The Ombud's office's finalized Privacy Breach Report Form will be submitted to the Superintendent before sending.	
4	Documenting the Breach	In consultation with the RTIPPA Coordinator, the supervising District or School Administrator shall complete the Privacy Breach Incident Report. This process may require: ○ Gathering and preserving all evidence relating to the breach. ○ Interviewing and securing written statements and/or notes of individuals with information relevant to the breach; ○ Obtaining all copies of all relevant documentation (written, electronic or recordings); ○ Documenting any procedures or practices of parties involved that do not appear in writing; ○ Identifying the individuals, both internal and external, who must be made aware of the breach and that the investigation is underway; and ○ Consulting with external resources, where and when appropriate.	RTIPPA Coordinator, Supervising District or School Administrator, ASD-W Staff
5	Evaluating the Breach	The RTIPPA Coordinator will assess the cause and extent of the breach, including the potential harm to the affected individual(s) resulting from the breach. The RTIPPA Coordinator determines if a privacy violation occurred and if the affected individual(s) and/or the Ombud needs to be notified.	RTIPPA Coordinator
6	Identifying Corrective Measures	Once the breach has been contained and remedied, it is important to identify corrective measures to prevent future breaches of the same or similar nature.	RTIPPA Coordinator, Supervising District or

		These measures could be, as appropriate: ○ An audit of the technical and physical security; ○ A review of policies and procedures and recommending revisions to reflect lessons learned from the investigation; ○ A review of employee training practices and recommendations; ○ A review of the existing practices of services delivery partners and agents; and ○ Any other measures considered by the Supervisor/ Director to be appropriate in the circumstances. As required, this analysis will be undertaken by the supervising District or School Administrator, the RTIPPA Coordinator, and other relevant staff.	School Administrator, ASD-W Staff
7	Closing the File	Once the breach has been evaluated, the RTIPPA Coordinator will submit the final Privacy Breach Report to the superintendent and district or school administrator involved. Depending on the severity of the breach, the report may also be sent to the other senior administrators. The breach will be logged in the Privacy Breach Incident Log.	RTIPPA Coordinator