ANGLOPHONE WEST SCHOOL DISTRICT

POLICY NO. ASD-W-801-1A

PRIVACY POLICY APPENDIX A

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

PRIVACY BREACH PROTOCOL

All suspected or actual privacy breaches whether they involve personal information or personal health information must be reported immediately to the direct supervisor, who will immediately report the actual/suspected breach to ASD-W Director of Communications who manages all matters related to the Right to Information and Protection of Privacy Act (RTIPPA).

The process to follow in the event that a breach has occurred is as follows:

- report an actual or suspected breach
- contain and mitigate the breach
- investigate the breach
- notify all potentially affected identified individuals
- issue a privacy breach report
- log the breach and corrective measures

*Note: These steps can be undertaken simultaneously.

Reporting an actual or suspected Privacy Breach

When an employee of the district, and/or third-party service provider is aware that a privacy breach has occurred, or is suspected to have occurred, that person must immediately notify their direct supervisor who will, in turn, notify the ASD-W Director of Communications. ASD-W email should be used to report a privacy breach and include “request a delivery receipt” for timeline tracking purposes.

If the breach involved an employee of the school district third-party service provider, the employee must notify the supervisor who liaises with the district. The district employee receiving a notification must notify their direct supervisor who will notify the ASD-W Director of Communications.

Containing and mitigating the breach

The ASD-W Director of Communications, in consultation with the individual(s) who discover(s) the breach will determine how to appropriately contain the breach.

Depending on how the breach occurred, and the severity of the breach, different steps for mediation can be taken, which may include:

- stopping the unauthorized practices;
- recovering the records and **all** copies;
- shutting down the system that has been impacted by the breach;
- revoking or changing computer access codes; and
- correcting the weakness in physical and/or electronics security.

Once the breach has been identified, reported, and contained (if applicable) the extent and scope of the breach must be assessed to determine the harm that has or could emanate from the breach.

Investigating the breach

Upon being notified of a suspected or actual breach, the ASD-W Director of Communications shall immediately undertake an investigation to:

- determine the scope (cause and extent) of the breach;
- determine the type and amount of information that was involved;
- gather evidence, including written statements and notes from all staff and all copies of all relevant documentation (written, electronic, or recordings);
- document any procedures or practices of parties involved that do not appear in writing;
- consult with external resources, if necessary; and
- recommend immediate actions to contain/mitigate the breach.

If the breach appears to involve theft or other criminal activity, the ASD-W Director of Communications, in consultation with the appropriate direct supervisor, will immediately contact the police and notify relevant staff of this action.

The ASD-W Director of Communications, in consultation with relevant staff, will assess the following components associated with the breach:

- what information was involved;
- the cause and extent of the breach;
- the individuals directly and indirectly affected by the breach;
- the foreseeable harm from the breach; and
- whether the immediate remedial actions were effective and sufficient to contain and mitigate the breach.

Where the services of a service provider are implicated in the event, related contracts should be reviewed to ensure that they provide an appropriate level of protection for the personal information and personal health information entrusted to that service provider and effective options for recourse to address a breach.

Any additional steps that are deemed necessary to further contain and remedy the breach should be taken at this time.

Notifying Affected Individuals

In keeping with the principles of openness and transparency, in the event of a breach of personal information and/or personal health information. ASD-W shall (except in accordance with exceptions outlined in the *Right to Information Protection of Privacy Act* and *Personal Health Information Protection and Access Act, where* notification is deemed inappropriate) notify all persons whose privacy was breached.

ANGLOPHONE WEST SCHOOL DISTRICT

POLICY NO. ASD-W-801-1A

PRIVACY POLICY APPENDIX A

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

The ASD-W Director of Communications, in consultation with the appropriate direct supervisor, and other relevant staff, will determine the scope of the notification:

- whether notification should occur;
- the mechanism for notification (direct mail and/or phone, public notice, media, internet, etc.);
- what should be included in the notification;
- when should the notification occur; and
- who should notify the affected individuals.

Concerns raised by the individual upon notification should be addressed as fully as possible; including, within reason, exploring additional corrective measures, and suggesting they also have the option to contact the Office of the Ombud for New Brunswick, Access and Privacy Division.

Issuing a Privacy Breach Report and notifying the Office of the Ombud

Once the breach has been contained and remedied, and the risk assessment is undertaken, ASD-W will issue a Privacy Breach Report using the Privacy Breach Reporting Form from the New Brunswick Office of the Ombud, Access and Privacy Division, found here:

Privacy-Breach-Reporting-Form-RTIPPA-ENG-Jan-2020.pdf (ombudnb-aip-aivp.ca)

The report will recommend corrective measures to help reduce the likelihood of future breaches of the same or similar nature. These messages could be, as appropriate:

- a review of policies and procedures and a recommendation of revisions to reflect lessons learned from the investigation;
- a review of employee training practices and recommendations;
- a review of the existing practices of service delivery partners and agents; and
- any other measures considered by the appropriate Director to be carried out in the situation.

The report may be submitted to the ASD-W Superintendent and EECD Policy and Planning Executive Director for their comments.

If the breach is deemed to have caused “significant harm” as defined by RTIPPA Regulation, the report will then be sent to Office of the Ombud for New Brunswick, Access and Privacy Division

- By fax: 506-453-5963
- By email: aip-aivp@gnb.ca
- By mail: 230 – 65 Regent Street, Fredericton, NB E3B 7H8
- For questions and inquiries call: 506-453-5965 or 1-877-755-2811 (toll free)

ANGLOPHONE WEST SCHOOL DISTRICT

POLICY NO. ASD-W-801-1A

PRIVACY POLICY APPENDIX A

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

Logging the breach and corrective measures

As required by RTIPPA regulation, ASD-W will maintain a registry of every actual and suspected privacy breach reported and include a list of corrective measures taken to reduce the likelihood of a similar breach from happening again.