AP 1202: Critical Incident and Privacy Breach

Background:

The Board of Education of School District No. 8 (Kootenay Lake) is committed to ensuring the protection and security of all personal information within its control. That commitment includes responding effectively and efficiently to privacy breach incidents that may occur.

The purpose of this procedure is to set out the School District's process for responding to significant privacy breaches and to complying with its notice and other obligations under the *Freedom of Information and Protection* of *Privacy Act* (FIPPA).

All staff of the School District are expected to be aware of and follow this Procedure in the event of a privacy breach. This Procedure applies to all employees, contractors and volunteers of the School District **("Staff")**.

The administration of this Procedure is the responsibility of the Superintendent/CEO of the School District, who is the "head" of the School District for all purposes under FIPPA (the "**Head**"). The Head may delegate any of their powers under this Procedure or FIPPA to other School District Personnel by written delegation.

Definitions:

Head: The Superintendent/CEO and includes any person to whom the Head has delegated their powers by written instrument.

Personal information: Any recorded information about an identifiable individual that is within the control of the School District and includes information about any student or any Staff member of the School District. Personal Information does not include business contact information, such as email address and telephone number, that would allow a person to be contacted at work.

Privacy Breach: The theft or loss of or the collection, use or disclosure of Personal Information not authorized by FIPPA, and includes cyber and ransomware attacks and other situations where there are reasonable grounds to believe that any such unauthorized activities have taken place or there is a reasonable belief that they will take place.

Privacy Officer: The person designated by the Head as Privacy Officer for the School District.

Records: Books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or other mechanism that produces records.

Staff: The employees, contractors, and volunteers of the School District.

Procedures:

1. Responsibilities of Staff:

    1.1. All staff must without delay report all actual, suspected or expected Privacy Breach incidents of which they become aware in accordance with this Procedure. All Staff have a legal responsibility under FIPPA to report Privacy Breaches to the Head.

    1.2. Privacy Breach reports may also be made to the Privacy Officer, who has delegated responsibility for receiving and responding to such reports.

    1.3. If there is any question about whether an incident constitutes a Privacy Breach or whether the incident has occurred, Staff should consult with the Privacy Officer.

    1.4. All Personnel must provide their full cooperation in any investigation or response to a Privacy Breach incident and comply with this Procedure for responding to Privacy Breach incidents.

    1.5. Any member of Staff who knowingly refuses or neglects to report a Privacy Breach in accordance with this Procedure may be subject to discipline, up to and including dismissal.

2. Privacy Breach Response:

    2.1. **Step One** – Report and Contain- Upon discovering or learning of a Privacy Breach, all Staff shall immediately report the Privacy Breach to the Head or to the Privacy Officer and take any immediately available actions to stop or contain the Privacy Breach, such as:

        2.1.1. Isolating or suspending the activity that led to the Privacy Breach; and

        2.1.2. Taking steps to recover Personal Information, Records or affected equipment.

        2.1.3. Preserving any information or evidence related to the Privacy Breach in order to support the School District's incident response.

        2.1.4. Upon being notified of a Privacy Breach the Head or the Privacy Officer in consultation with the Head, shall implement all available measures to stop or contain the Privacy Breach. Containing the Privacy Breach shall be the first priority of the Privacy Breach response, and all Staff are expected to provide their full cooperation with such initiatives

    2.2. **Step Two** – Assessment and Containment- The Privacy Officer shall take steps to, in consultation with the Head, contain the Privacy Breach by making the following assessments:

2.2.1. The cause of the Privacy Breach;

2.2.2. If additional steps are required to contain the Privacy Breach, and, if so, to implement such steps as necessary;

2.2.3. Identify the type and sensitivity of the Personal Information involved in the Privacy Breach, and any steps that have been taken or can be taken to minimize the harm arising from the Privacy Breach;

2.2.4. Identify the individuals affected by the Privacy Breach, or whose Personal Information may have been involved in the Privacy Breach;

2.2.5. Determine or estimate the number of affected individuals and compile a list of such individuals, if possible; and

2.2.6. Make preliminary assessments of the types of harm that may flow from the Privacy Breach.

2.2.7. The Head, in consultation with the Privacy Officer, shall be responsible to, without delay, assess whether the Privacy Breach could reasonably be expected to result in significant harm to individuals. That determination shall be made with consideration of the following categories of harm or potential harm:

2.2.7.1. Bodily harm;

2.2.7.2. Humiliation;

2.2.7.3. Damage to reputation or relationships;

2.2.7.4. Loss of employment, business or professional opportunities;

2.2.7.5. Financial loss;

2.2.7.6. Negative impact on credit record;

2.2.7.7. Damage to, or loss of, property;

2.2.7.8. The sensitivity of the Personal Information involved in the Privacy Breach; and

2.2.7.9. The risk of identity theft

2.2.7.10. Reference to social media

2.3. **Step Three** – Notification - If the Head determines that the Privacy Breach could

reasonably be expected to result in Significant Harm to individuals, then the Head shall make arrangements to:

2.3.1. Report the Privacy Breach to the Office of the Information and Privacy Commissioner; and

2.3.2. Should provide notice of the Privacy Breach to affected individuals, unless the Head determines that providing such notice could reasonably be expected to result in grave or immediate harm to an individual's safety or physical or mental health or threaten another individual's safety or physical or mental health.

2.3.3. If the Head determines that the Privacy Breach does not give rise to a reasonable expectation of Significant Harm, then the Head may still proceed with notification to affected individual if the Head determines that notification would be in the public interest or if a failure to notify would be inconsistent with the School District's obligations or undermine public confidence in the School District.

2.3.4. Determinations about notification of a Privacy Breach shall be made without delay following the Privacy Breach, and notification shall be undertaken as soon as reasonably possible. If any law enforcement agencies are involved in the Privacy Breach incident, then notification may also be undertaken in consultation with such agencies.

2.4. **Step Four** – Prevention - The Head, or the Privacy Officer in consultation with the Head, shall complete an investigation into the causes of each Breach Incident reported under this Procedure, and shall implement measures to prevent recurrences of similar incidents.