AP 610-1 PRIVACY BREACH
POLICY #610

CARIBOO - CHILCOTIN SCHOOL DISTRICT

RATIONALE:

A privacy breach is a collection, use, disclosure, access, disposal of personal information, whether accidental or not, that is not authorized by the *British Columbia Freedom of Information and Protection of Privacy Act.*

A privacy breach can be accidental or deliberate and includes theft, loss, alteration, or destruction of personal information. "Personal Information" means information about an identifiable individual. The district is required to have a process for responding to a privacy breach and advising employees of their responsibility to report any actual or suspected privacy breach incidents.

PROCEDURE:

1. Roles and Responsibilities

1.1 In accordance with the *Freedom of Information and Protection of Privacy Act*, all district employees must immediately report any actual or suspected privacy breach incidents to their Principal/supervisor in accordance with this procedure.

1.2 The Secretary Treasurer is the designated FOIPPA Officer for the district. The FOIPPA Officer or their designate is responsible for all investigations and subsequent documentation in relation to any reported privacy breach incidents. All reported incidents will be documented along with any action taken. The FOIPPA Officer will assess whether the reported incident requires immediate action to prevent any recurrence of a similar incident.

2 Privacy Breach Response Process

2.1 Employees

Upon becoming aware of an actual or suspected privacy breach, all district employees shall:

2.1.1 immediately report the suspected or actual breach to their Principal/supervisor; and

2.1.2 take action, where possible, to contain the breach and limit its impact by:

2.1.2.1 isolating or suspending the activity that led to the privacy breach;

2.1.2.2 taking immediate steps to recover the personal information, records, or equipment where possible; and

2.1.2.3 determining if any copies have been made of the personal information at risk and recovering where possible.

2.2 Principal/Supervisor

Upon being notified of an actual or suspected privacy breach, the Principal/supervisor shall:

2.2.1 immediately notify the FOIPPA Officer of the breach and work with the FOIPPA Officer or their designate to carry out a preliminary assessment of the extent and impact of the privacy breach, including:

2.2.1.1 assess whether additional steps are required to contain the breach, implementing as necessary;

2.2.1.2 identify the type and sensitivity of personal information breached and any steps that have been taken to minimize the harm from the breach;

2.2.1.3 identify who is affected by the breach;

2.2.1.4 estimate the number of individuals affected by the breach;

2.2.1.5 identify the cause of the breach; and

2.2.1.6 identify foreseeable harm from the breach.

2.3 FOIPPA Officer

The FOIPPA Officer or designate shall be responsible for the detailed investigation of incidents of actual or suspected privacy breaches. The FOIPPA Officer's investigation shall include but not be limited to:

2.3.1 assessing all information reported by the Principal/supervisor and obtaining further clarification of events and findings if required;

2.3.2 taking any further steps required to minimize or reduce the harm; and

2.3.3 assessing foreseeable harm from the breach including but not limited to:

2.3.3.1 risk of harm to the individual(s);

2.3.3.2 loss of public trust in the district;

2.3.3.3 risk to public safety; and,

2.3.3.4 financial exposure.

3 District Actions and Notifications

3.1 The determination of whether to notify individuals, public bodies, organizations affected by the privacy breach, or the Privacy Commissioner, will be made by the FOIPPA Officer. The considerations shall include but are not limited to:

3.1.1 necessity to avoid or mitigate harm to the affected individual, public body or organization;

3.1.2 legislative requirements;

3.1.3 contractual obligations;

3.1.4 potential risk of identity theft or fraud due to the breach of any personal identification information;

3.1.5 any risk of physical harm due to the privacy breach such as stalking or harassment;

3.1.6 a risk of damage to reputation, hurt or humiliation such as when the privacy breach includes the release of medical or disciplinary information;

3.1.7 a risk of loss or business or employment opportunities should the privacy breach result in damage to the reputation of an individual; and

3.1.8 a risk of the loss of confidence in the district, or any related public body or organization, and good district relations.

3.2 If notification of individuals is determined to be necessary, the notification should occur by the direct Principal/supervisor or designate as soon as possible following the breach. If a law enforcement agency has been informed of the breach, and is conducting a criminal investigation, consultation and cooperation should occur in order to facilitate the investigation.

3.3 Where feasible, affected individuals will be notified directly, by the direct Principal/supervisor or designate by phone, email, letter or in person, depending upon the practicalities. Indirect notification using general, non-personal information will usually occur only when direct notification could cause further harm, is prohibitive in cost, or contact information is unavailable. In some circumstances, using multiple methods of notification may be considered.

3.4 If the FOIPPA officer determines notification of the privacy breach is not required, documentation of the rationale must be recorded and maintained by the officer.