AP 148 - Privacy Breach

Background

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 the theft, loss, alteration or destruction of personal information. "Personal Information" means information about an identifiable individual.

School District No. 45 (West Vancouver) is required to have a process for responding to a privacy breach in accordance with the *British Columbia Freedom of Information and Protection of Privacy Act*.

1. Roles and Responsibilities

1.1 All district employees must immediately report any actual or suspected privacy breach incidents to their administrator/manager in accordance with this Administrative Procedure.

1.2 The Secretary-Treasurer is the designated FOI Officer for the district. The FOI Officer or their designate is responsible for all investigation and subsequent documentation in relation to any reported privacy breach incidents. All reported incidents will be documented along with any action taken. The FOI 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 Responsibilities of Employee: 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 supervisor/manager/administrator;

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

- Isolating or suspending the activity that led to the privacy breach
- Taking immediate steps to recover the personal information, records, or equipment where possible;
- Determining if any copies have been made of the personal information at risk and recovering where possible

2.2 Responsibilities of Supervisor/Manager/Administrator: Upon being notified of an actual or suspected privacy breach, the supervisor/manager/administrator shall:

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

- Assessing whether additional steps are required to contain the breach, implementing as necessary;
- Identifying the type and sensitivity of personal information breached and any steps that have been taken to minimize the harm from the breach;
- Identifying who is affected by the breach;
- Estimating the number of individuals affected by the breach;
- Identifying the cause of the breach; and
- Identifying foreseeable harm from the breach.

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

3.1 Assessing all information reported by the supervisor/manager/administrator and obtaining further clarification of events and findings if required;

3.2 Taking any further steps required to minimize or reduce the harm;

3.3 Assessing foreseeable harm from the breach including but not limited to:

- Risk of harm to the individual(s);
- Loss of public trust in the district;
- Risk to public safety;
- Financial exposure;

4. District Actions and Notifications:

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

- Necessity to avoid or mitigate harm to the affected individual, public body or organization;
- Legislative requirements;

- Contractual obligations;
- Potential risk of identity theft or fraud due to the breach of any personal identification information;
- Any risk of physical harm due to the privacy breach such as stalking or harassment;
- A risk of damage to reputation, hurt or humiliation such as when the privacy breach includes the release of medical or disciplinary information;
- A risk of loss of business or employment opportunities should the privacy breach result in damage to the reputation of an individual;
- A risk of the loss of confidence in the district, or any related public body or organization, and good district relations.

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

4.3 Where feasible, affected individuals will be notified directly, by the direct supervisor/manager/administrator 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.