BOARD OF EDUCATION OF
SCHOOL DISTRICT NO. 46 (SUNSHINE COAST)

POLICY COMMITTEE
AGENDA

Tuesday, October 25, 2016 from 11:30-1:00 p.m.
School Board Office – Gibsons, BC

---

1) Trustee Volunteering Policy

2) Trustee Email Policy

3) Whistleblower Policy

Volunteers
Policy 2150
May 26, 2015

The Board of Education believes that community volunteers can make valuable contributions to the education of students. The Board believes that the use of volunteers supports parental involvement, complements the skills and expertise of employees, assists schools in providing enriching, learning experiences and extracurricular programs, and strengthens lines of communication among the school, home, and community.

It is the intent of the Board to comply with the provisions of collective agreements, including those provisions which restrict the use of volunteers.

The Board expects that school volunteers will be selected, oriented, and supervised in order to minimize risk to students, maximize contribution to realizing School District objectives, and to ensure the protection of the privacy of students, their families and all student records.

Guidelines

1. The Principal and/or Vice-Principal shall ensure that adequate safety precautions are in place.

    1.1 Volunteers will be supervised by an employee of the Board who is familiar with District policies and codes of conduct.

    1.2 Volunteers shall not be permitted to have their non-enrolled or non-participating children accompany them during structured instructional activities. (Notwithstanding Field Trips Policy 6220 Section 4.2.5.1)

    1.3 The Principal and/or Vice-Principal will complete a community volunteer form during a meeting with the volunteer.

    1.4 The Volunteer will receive information regarding school expectations.

    1.5 The Volunteer will complete the authorization for a criminal record check through the local RCMP office.

    1.6 The Principal and/or Vice-Principal will contact 2 local references.

    1.7 The Principal and/or Vice-Principal will review pertinent information, make the decision regarding approval, and notify the applicant of the decision to approve or not approve the application.

    1.8 Complaints about volunteers will be handled confidentially by the Principal and/or Vice-Principal, in consultation with the Superintendent.

    1.9 A volunteer's services may be terminated at the discretion of the Principal and/or Vice Principal, in consultation with the Superintendent.

Expectations of Volunteers

2. Volunteers must:

2.1 adhere to the bylaws, policies, and regulations of the Board;

2.2 speak and act toward students, parents, staff, and other volunteers with respect;

2.3 respect complete confidentiality with regard to all students, personnel, and school matters;

2.4 report all incidents of student or others' personal injury to staff;

2.5 promptly report to the Principal, Vice-Principal or Superintendent if charged with or convicted of a relevant offense subsequent to a criminal record check.

720R – VOLUNTEERS
(REGULATIONS)

1. Definition

For the purpose of this policy, the term "volunteers" shall be adult persons (age 19 years or over) other than employees who:

1.1 willingly provide services to schools without expectation of compensation;

1.2 may attend at the school one time only, occasionally, or on a regularly scheduled basis;

1.3 may have an assigned role or responsibility in a school, classroom, or during a school activity.

2. Recruitment

Inviting, accepting, assigning and training volunteers are carried out at the school level. Individuals interested in serving as volunteers must contact the school principal. District-wide protocols and volunteer application forms shall be used.

3. Role of the Principal

It is the responsibility of the school principal to:

3.1 Ensure that all volunteers are advised that they will be required to submit to a criminal record check prior to volunteering at the school. (Note: Criminal record checks completed for other organizations are not valid for the School District.)

3.2 Ensure the criminal record checks for volunteers are completed, through the school district, when the volunteer begins with the district, and again after four years if the individual continues as a volunteer. (Note: Criminal record checks are valid for five years but due to the processing time, continuing volunteers are required to complete a criminal record check at least every four years.)

3.3 Provide for the safety of students in the care of volunteers;

3.4 Monitor the activities of the volunteers;

3.5 Implement the appropriate provisions of the collective agreements.

3.6 Ensure the completion of and compliance with Form 525.3 if transporting students in their private vehicles.

4. Liability

Volunteers selected by these regulations will be covered by the district's liability insurance plan.

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Use of Personal Email Accounts for Public Business

Introduction

This document explains the implications under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") for use of personal email accounts for work purposes by employees of public bodies. It conveys two key messages. First, FIPPA applies to the use of personal email accounts for work purposes. Second, public bodies should not, for FIPPA purposes, allow the use of personal email accounts for work.

Application of FIPPA to Personal Email Accounts

FIPPA applies to all records in the custody *or* under the control of a public body. Email are records under FIPPA.[1] Records are in the custody of a public body if it has "charge and control" of the records, "including some legal responsibility for their safekeeping, care, protection or preservation."[2] While the public body would have custody of email residing on its server, it would not have custody for personal email residing elsewhere. The issue in such cases would be whether personal email is under the control of a public body.

The use of personal email accounts for work purposes can give the perception that public body employees are seeking to evade the freedom of information process.

The Supreme Court of Canada has said that where a record is not in the physical possession of a government institution, it will still be under its control if these two questions are answered in the affirmative:

[1] See s. 3(1) of FIPPA.
[2] See para. 23 of Order 02-30, [2002] B.C.I.P.C.D. No. 30 and p. 9 of Order No. 308-1999, [1999] B.C.I.P.C.D. No. 21.

(1) Do the contents of the document relate to a departmental matter?

(2) Could the government institution reasonably expect to obtain a copy of the document upon request?[3]

The facts of each case will determine whether personal email are under the control of a public body. As a general rule, any email that an employee sends or receives as part of her or his employment duties will be a record under the public body's control, even if a personal account is used.

ADEQUATE SEARCH (S. 6(1) OF FIPPA)

FIPPA requires public bodies to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely. This includes a duty to perform an adequate search for records that respond to an access request. A public body must be able to prove that its search efforts have been thorough and comprehensive and that it has explored all reasonable avenues to locate records.[4] The Information and Privacy Commissioner has the authority to compel the production of records in the custody or under the control of a person[5], including those in personal email accounts.

The use of personal email accounts by employees does not remove or reduce the duty of a public body to search for records and produce those that are responsive to an access request.

The use of personal email accounts does not relieve public bodies of their duty to comprehensively search for requested records and to produce them. While nothing in FIPPA directly prohibits public body employees from using personal email accounts, doing so may make it more difficult for their employer to search for records. Employees may be unwilling to produce records from their personal account or to allow access to their accounts for that purpose.

To address this risk, public bodies should create policy on the use of personal email accounts for work purposes. A preferred solution is for public bodies to require the use of its email system for work purposes. If that is truly not practicable, the policy should be that employees must copy their work email account on any work-related email they send from a personal account.[6] This policy should be part of each employee's conditions of employment.

---

[3] See *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25.
[4] See, for example, Order F07-12, [2007] B.C.I.P.C.D. No. 17, Order 00-32, [2000] B.C.I.P.C.D. No. 35 and Order 00-26, [2000] B.C.I.P.C.D. No. 29.
[5] See s. 44(1)(b) of FIPPA.
[6] This policy should also apply where there is a ban on use of personal email accounts for work purposes, to deal with cases where an employee failed to comply with the policy and possesses personal email that might be responsive to an access to information request.

REASONABLE SECURITY MEASURES (S. 30 OF FIPPA)

Another risk relates to security of personal information. FIPPA requires public bodies to take reasonable security measures to guard against unauthorized access, collection, use, disclosure or disposal of personal information. A personal email account, which is often web-based, is much less likely to comply with this requirement than a public body's email system. First, the terms of service for personal accounts may allow third-party access to content in a way that is in contravention of FIPPA. Second, security features for webmail services may not be adequate for FIPPA purposes. Any public body that allows use of personal email accounts to send or receive personal information is therefore risking non-compliance with FIPPA.

Storage and Access must be in Canada (s. 30.1 of FIPPA)

Although there are exceptions, including consent by affected individuals, [7] FIPPA requires public bodies to store and access personal information only in Canada. Public bodies have to assume that webmail resides on servers outside Canada, at least some of the time. This presents a serious risk of non-compliance for public bodies that allow use of personal email that contains personal information.

Disclosure Outside of Canada (s. 33.1 of FIPPA)

FIPPA prohibits the disclosure of personal information outside of Canada unless authorised by s. 33.1. The use of a webmail service that has servers outside of Canada will almost certainly result in public bodies disclosing personal information outside of Canada. Unless s. 33.1 authorizes the disclosure, use of webmail to send or receive personal information would violate FIPPA.

RESPONSIBLE INFORMATION MANAGEMENT

The citizens of British Columbia expect accountability from public bodies in their actions as well as their information practices. One important way for public bodies to demonstrate this accountability is to create an accurate record of actions in a manner that preserves records of enduring value. When employees of public bodies conduct business through their personal email accounts, accountability is easily lost.

[7] See s. 11(2)(b) of the Freedom of Information and Protection of Privacy Regulation. The rules for obtaining consent mean that public bodies will rarely be authorized to use personal email accounts.

CONCLUSION

FIPPA applies to work-related email sent to or received from the personal email accounts of public body employees. This document shows how use of personal email accounts for work purposes presents several challenges for public bodies under FIPPA. As indicated above, for FIPPA purposes, public bodies should not allow use of personal email accounts to conduct public business. They should ensure that clear policy is in place in this area and that all employees agree to comply with the policy.

If you have any questions about this document, please contact us at:

Office of the Information and Privacy Commissioner for BC
Tel: (250) 387-5629 (in Vancouver call (604) 660-2421)
Elsewhere in BC call 1-800-663-7867
Email: info@oipc.bc.ca

SD 42 POLICY: 7110

WHISTLE BLOWER PROTECTION

PHILOSOPHY

The Board of Education ("Board") is strongly committed to upholding ethical standards in the School District and will foster and maintain an environment where employees can work safely and appropriately without fear or retaliation. All employees, and others performing work on behalf of the School District, are expected to conduct themselves in a professional manner, adhere to applicable laws and Board Policies and Procedures that apply to their work activities in addition to demonstrating ethical behavior in all their decisions and interactions.

The Board expects employees, and others that we deal with, who have serious concerns about any aspect of the School District's operations with respect to potential evidence of wrongdoing, to come forward and voice those concerns.

AUTHORITY

The responsibility for the day to day administration and enforcement of this Policy rests with the Superintendent of Schools and the Secretary Treasurer as authorized by the Board of Education. Reports of workplace wrongdoings may be made to the Board Chairperson or with the Superintendent or Secretary Treasurer.

The provisions of this Policy are independent of, and supplemental to, the provisions of collective agreements between the School District and its Unions relative to grievance procedures and to any other terms and conditions of employment.

POLICY VIOLATIONS

It is a violation of the Policy for anyone to knowingly make a false complaint of wrongdoing or to provide false information about a complaint. Individuals who violate this Policy are subject to disciplinary and/or corrective action, up to and including termination of employment.

APPROVED: May 30, 2012

SCHOOL DISTRICT NO. 36 (SURREY)

No. 7110

POLICY: WHISTLE BLOWING

Philosophy

The Board is strongly committed to upholding ethical standards in the School District. All employees, and others performing work on behalf of the District, are expected to conduct themselves in an ethical and professional manner, to adhere to applicable laws and Board Policies & Regulations and to report in good faith any wrongful conduct in connection with the District's operations.

This Policy is intended to encourage and support employees throughout the District to act with integrity. Employees and other individuals who have dealing with the School District, including parents, volunteers and contracted service workers may access the processes under this Policy to report wrongful conduct.

Authority

The responsibility for the day to day administration and enforcement of this Policy rests with the Superintendent of Schools and the Secretary-Treasurer.

This Policy is independent of, any collective agreements or written employment agreements between the District and its employees and any grievance procedures or dispute resolution processes contemplated in such agreements.

Revised: 2016-06-03
Approved: 2009-06-25