Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

# Top 10 Tips for Elected Officials for Complying with FOI and Privacy

1. Since 1994, municipalities and regional districts have been subject to the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The purposes of FIPPA are to protect privacy and to make public bodies more accountable. It applies to all records in the custody or under the control of the municipality.

2. Officers of a public body who have access to personal information must not disclose personal information unless authorized by FIPPA. The term "officers" in FIPPA includes all municipal Councillors, Mayors and Regional District Directors (*R. v Skakum,* 2012 BSCS 1103).

3. Emails and other documents generated in your work for your municipality could be the subject of an FOI request. Keep personal email separate from municipal business. Do not use your personal email account to conduct municipal business. (See Hilary Clinton and email use scandal).

4. All personal information in the custody or control of a public body must be stored in Canada. This is another reason not to use personal email accounts for municipal business – they likely store your information outside of Canada.

5. As a municipal official you may have access to information that you do not need for your work. It is unlawful to browse for information about anyone without a direct business purpose. Best practice is that you will only be given access to the information that you require to perform your specific role.

6. If you receive or collect personal information as an elected official doing business for your local government, you must be aware that FIPPA limits how you may use or disclose that information, even after you have left public office.

7. Personal information stored electronically on laptop computers, USB drives or other mobile devices must be encrypted. Do not leave laptops or other mobile devices unattended in motor vehicles. Keep personal information under lock and key when not in use.

8. Activities that are not related to local government business, such as campaigning activities, are not subject to the access provisions of FIPPA. However, if records relate to campaigning and contain personal information, they may be subject to the privacy provisions of the *Personal Information Protection Act* for which the candidate is personally accountable.

9. Best practice is to have all new elected officials participate in mandatory access and privacy training. The OIPC has partnered with service providers to provide approved training on a fee for service basis.

10. Each municipality has an FOI and Privacy Officer. Part of their job is to answer your questions and provide you with advice. Please consult them. If a constituent sends an FOI request directly to you, forward it immediately to the FOI Officer.

## OTHER USEFUL MATERIALS

### *Investigation Reports*

IR F15-01 Use of Employee Monitoring Software by the District of Saanich

IR F13-05 Public Body Disclosure of Information under Section 25 of the Freedom of Information and Protection of Privacy Act

### *Special Reports*

July 22, 2014: A Failure to Archive: Recommendations to Modernize Government Information Management

Aug. 30, 2006: Local Governments and the Growth of Surveillance

### *Guidance Documents*

March 18, 2013: Use of Personal Email Accounts for Public Business

April 17, 2012: Getting accountability right with a privacy management program & At-a-glance document

Feb. 23, 2012: Cloud computing for public bodies