

Controlling Internal Access To Local Government Records

by Lorena Staples QC
January 2003

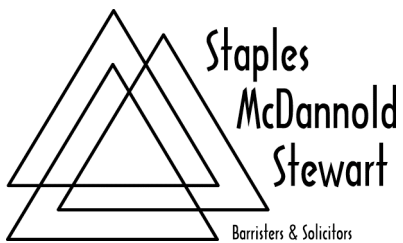


Table of Contents

Introduction	1
Issues.....	2
Common Law Right to Access.....	3
Statutory Right to Access	4
Officer Status.....	5
Personal Information.....	6
Business Information	7
Information Necessary to Discharge Duties.....	8
Access According to Role.....	9
Implications of Section 198 of the Local Government Act.....	10
Off-site Access	11
Recommendations	12
Summary.....	14

What access to municipal records are local government elected officials and employees entitled to as a result of their official positions? What are the implications if elected officials receive their weekly agenda packages, including attachments and reports, electronically by way of either e-mail or the local government's internet web site? This paper addresses the propriety of off-site access to the records, as well as general access at the local government's offices.

There are two distinct issues relating to a local government's corporate records and the ability of both employees and elected officials to have access to them:

1. The extent to which elected officials and employees have the right to access the information.
2. The duties and responsibilities of all those, including elected officials and employees, who have access to all or some of the records of the local government.

Common Law Right to Access

Local government elected officials and employees have the right of access to local government records, in common with other members of the public under the Freedom of Information and Protection of Privacy Act (FOIPPA). However, it is not that type of access that is at issue here: it is the access to and, in some cases, the possession of municipal records that flows from the fact of being elected to or employed by the local government. That is not a right of access held in common with members of the public generally.

Statutory Right to Access

There is a limited statutory right to the disclosure of personal information by a public body under section 33(f) of FOIPPA. That section states that:

A public body may disclose personal information only to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister.

In the context of these issues, we must consider if an elected official is an officer for the purposes of section 33(f) before determining if the elected official needs the information for the performance of that person's duties.

There is no definition of "officer" in FOIPPA, the Local Government Act or the Interpretation Act. In section 287 of the Local Government Act the term "municipal public officer" is defined to include an elected official as well as an officer or employee of a local government, but that section is for the sole purpose of providing a statutory immunity to all of the defined persons from actions for damages under certain circumstances. It does not confer the status of "officer" on those persons for other purposes

Part 5.1 of the Local Government Act provides for the appointment of the statutory officers of a local government, as well as other types of officers. Also, under Part 5.2 relating to municipal councils, section 209 deals with the term of office for council members and section 210 with the oath of office for them. They can be disqualified from office under section 211 or resign from office under section 212. Similar provisions for the office of regional board directors are found in sections 784 and 785. Therefore, it is abundantly clear that regional board directors, municipal councillors and mayors are considered officers of the local government. They are elected to an office; they are not hired as employees. Therefore, all members of Council are officers for the purpose of section 33(f) of FOIPPA.

Personal Information

Section 33(f) refers to the disclosure of personal information. "Personal information" is defined in Schedule 1 of FOIPPA as follows:

"personal information" means recorded information about an identifiable individual, including

- (a) the individual's name, address or telephone number,
- (b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- (c) the individual's age, sex, sexual orientation, marital status or family status,
- (d) an identifying number, symbol or other particular assigned to the individual,
- (e) the individual's fingerprints, blood type or inheritable characteristics,
- (f) information about the individual's health care history, including a physical or mental disability,
- (g) information about the individual's educational, financial, criminal or employment history,
- (h) anyone else's opinions about the individual, and
- (i) the individual's personal views or opinions, except if they are about someone else.

As we can see, elected officials and other officers of a local government, as well as employees, have a limited right to access personal information in the control of the local government. It is not clear whether elected officials are entitled to access other types of information, such as the business information that is described in section 21 of FOIPPA. This type of information is often given to the local government because the person involved has an application before the local government that will ultimately find its way to the agenda. Elected officials may have to see that information as part of their decision making process.

There is an explicit set of circumstances described in section 21 that must occur before disclosure of the information is considered harmful to the business interests of a third party. The information must be supplied, implicitly or explicitly, in confidence, and must consist of trade secrets of that person, or commercial, financial, labour relations, scientific or technical information relating to that person.

In addition to the foregoing, the disclosure of that information must have been reasonably expected to harm significantly the competitive position or interfere significantly with the negotiating position of the party, or result in similar information no longer being supplied to the local government when it is in the public interest that similar information continues to be supplied.

Moreover, the disclosure must reasonably be expected to result in undue financial loss or gain to any person or organization, or reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

If the person consents to the disclosure of his or her information, then section 21 will not apply.

The limitations on disclosing business information illustrate the care that must be taken by all officers and employees of a local government in handling records containing information of all types.

Information Necessary to Discharge Duties

In considering the meaning of the words “if the information is necessary for the performance of the duties of an officer or employee” in section 33(f), we canvassed the case law to ascertain when information becomes necessary to the performance of a councillor’s duties, and found a number of cases from Britain, Quebec and Ontario on the issue of “need to know”.

In *H. (J.) D. Hastings (County)* (1992) 12 M.P.L.R. (2d) 40, an Ontario court was concerned specifically with personal information and found that in that case, the information must be necessary to the Councillors carrying out their duty. There were no duties for Council to carry out in that case, and therefore they were not entitled to the information.

The other cases dealt with general types of information, as well as personal information. The rule regarding the former is somewhat similar to the rule with respect to personal information. If the specific Councillor has no duties to perform with respect to the information, then it is not necessary for the Councillor to see the information. For example, if the Councillor was not on a committee dealing with the information, the Councillor had no right to see it.

The British cases make no reference to freedom of information legislation. They may no longer be relevant in light of the general right of access under BC’s FOIPPA. However, they are relevant in determining whether the personal information is required to perform a member’s duties, as set out in section 33 of FOIPPA. The application of those cases is summarized below and applies equally to municipalities and regional districts.

Access According to Role

1. Where a Council member is acting under the direction of Council as a whole, with regard to a specific task or issue, or acting in concert with Council or a committee of Council, then, under section 33 of FOIPPA, that member would have access to personal information, and business information (not given in confidence under section 21 of FOIPPA) where that information was supplied by the person to whom it relates for the purpose of that task.
2. A Council member acting as a constituent representative is acting as an advocate for that person, not in concert with Council as a whole, or as a member of an assigned committee or task force, and would have no greater access to information in the local government records than a member of the public would have. (see item 4)
3. A member who is acting on his/her own with no duties to perform as an elected official or on the direction or request of a constituent would have the same right of access as a member of the public under FOIPPA. (see item 4)
4. A member of the public does not have a right of access to personal information, business information under section 21 of FOIPPA or other information unless it is disclosable under FOIPPA.

Implications of Section 198 of the Local Government Act

Paragraph (b) of section 198 confers a duty on the corporate administrator to ensure that access is provided to records of the local government and its committees, as required by law or authorized by the local government. This is in addition to paragraph (a) where the corporate administrator must maintain and keep safe the minutes of meetings and the bylaws and other records of the business of the local government and its committees. Section 198(b) reflects the existence of FOIPPA by requiring the corporate administrator (formerly the clerk) to ensure that the records are accessible in accordance with FOIPPA rules.

The words “as required by law” in section 198(b) limit access to the access allowed under FOIPPA, the Local Government Act and other applicable legislation. The corporate administrator is not required to make any and all records available to any person, including elected officials and other employees of the local government. The section simply confers the responsibility for record keeping and access to records on the corporate administrator, but the right to access is still determined in the first instance by the designated “head” under FOIPPA.

The person designated as the “head” of the local government under FOIPPA is often the corporate administrator or an employee of that department, but could be employed in some other part of the administration.

Under section 30 of FOIPPA, the head of a public body must protect any personal information in the records of the local government by taking reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. If access to the local government's records is available within the local government's offices by elected officials and employees through the local government's intranet, this duty can be compromised unless steps are taken to preserve the confidentiality of the records.

Making personal information accessible to local government officials and employees on an off-site basis by means of portable laptop computers and other electronic devices poses security problems. The laptops may be accessible to other persons, including children, who have no understanding of the statutory protection afforded to the records. At a minimum, these devices should be password protected so that no other person can have access either to the computer or device itself, or, by extension, to the local government's records.

The same security problems apply to hard copies of records. If staff, Councillors or Board members take their own copies of sensitive documents containing personal information to their homes or outside offices, there is the risk these documents may fall into the hands of persons who are not authorized to see them. The local government will have failed in its duty to protect that information from disclosure.

To avoid security leaks, documents containing sensitive information can be made available in a very limited manner. Numbered copies can be distributed at meetings only rather than in advance. Then when council or board has dealt with the matter, the copies can be collected and either destroyed or stored in a secure place. Members needing the information in advance can view it in the corporate administration office.

1. Level of Access

There are various levels of access that can be given to elected officials, as well as to employees of the local government. It is understood that the limitation of access would have to be practical from a technical, as well as a convenience point of view.

Elected officials may need only the basic service of having their agenda packages, including attachments or reports, sent to them electronically by e-mail or available on the local government's intranet web site. A page of the web site can be dedicated to the agenda packages and can be password protected, giving the password only to elected officials and those staff that require it. The information should also be password protected on their home or business office computer.

If elected officials require additional information, their requests could be funneled through the Corporate Administrator or FOIPPA head, who could then determine whether they should have access to the additional information.

Sensitive information should be deleted from the web site once it has been dealt with by the council/board.

2. Security Arrangements

Section 30 of FOIPPA requires the head to protect personal information with reasonable security arrangements. Otherwise, there may be inadvertent contraventions of FOIPPA. If the local government fails to provide security for its records, it may be considered negligent and be subject to actions for damages. Note that section 73 of FOIPPA provides protection from such lawsuits but only where the public body or official was acting in good faith. Knowing that security should be provided and failing to act on that knowledge can be evidence of bad faith.

No one should be allowed the kind of access that allows them to take records outside of the local government offices without the necessary security precautions in place.

Computers in the local government offices should be secure from access by members of the public, as evidence of the local government's good faith efforts to protect personal and business information as required by FOIPPA. So-called "dumb" terminals can be set up for the public to view public records, such as bylaws.

Failure to take these steps could have serious repercussions for the local government in terms of financial penalties as well as loss of confidence by the public.

3. Training

If elected officials are given access to the local government's records, then they must be given specific instructions and training on how to handle the records, and especially on the disclosure rules under FOIPPA. A primary rule is that they should not give anyone else copies of the records or access to them. Determining who should have that access is the function of the FOIPPA head. The head determines in the first instance whether

access is available to specific local government records. Elected officials are not entitled by law to make those decisions.

The records handling training should be updated regularly and newly elected officials and new staff should be immediately trained in this regard before being given access to local government records.

To summarize, section 33 of FOIPPA gives members of Council and employees alike a right to access personal information but only if it is necessary for them to have the personal information in order to carry out their duties. Other types of information protected under FOIPPA and other Acts should not be disclosed and all persons, including elected officials and employees, who have access to local government records should be trained in the handling of this information and educated in the consequences to themselves and the local government if this information is disclosed.

No information should be given out or access provided to records without the approval of the FOIPPA head. The head is required to provide reasonable protection for the security of personal information. Off-site computer access should be password protected and on-site computers secured from access by unauthorized persons. Unlimited access carries the risk of inadvertent disclosure and even deliberate misuse of information, with financial and other consequences to the municipal corporation, its officers and employees.