

# ATTACHMENT B



<b>Section:</b>	<b>Administration</b>	<b>1</b>
<b>Subsection:</b>	<b>Information and Privacy</b>	<b>0580</b>
<b>Title:</b>	<b>Privacy Policy</b>	<b>01</b>

## REASON FOR POLICY

The purpose of the City of Nanaimo's Privacy Policy is to describe how the City collects, uses, discloses and protects personal information. This policy provides a framework for how the City will operate in order to ensure personal information is managed in accordance with the *Freedom of Information and Protection of Privacy Act*. This policy also gives examples of what personal information the City needs, and examples of how it uses and discloses personal information.

## SCOPE

This policy applies to personal information that the City collects, uses or discloses in any form (including verbal, electronic or written personal information).

This policy does not apply to any collection, use or disclosure of personal information through the City's website. The City's website privacy policy can be accessed through this link:

<https://www.nanaimo.ca/privacy-policy>

## DEFINITIONS

The following definitions are used in this policy:

- a. "Act" means the *Freedom of Information and Protection of Privacy Act* (British Columbia);
- b. "City" means the City of Nanaimo;
- c. "employee" means an employee of the City, including a volunteer;
- d. "personal information" means recorded information about an identifiable individual;
- e. "service provider" means a person we retain under a contract to perform services for us;
- f. "us" refers to the City, as do "our", "we" and similar terms, not to any employees or elected or appointed City officials;
- g. "you" refers to anyone whose personal information we collect, use or disclose

## POLICY STATEMENT

This policy is established in accordance with the City's *Freedom of Information and Protection of Privacy Act Bylaw 7024*. We protect the personal information we collect, use and disclose in accordance with the *Freedom of Information and Protection of Privacy Act (FIPPA)* by promoting privacy awareness, applying sound privacy principles and implementing reasonable security measures.

This policy is the foundation for the City's privacy management program. It sets the framework for privacy to be a central component of our business practices and a built-in component of our day-to-day program operations.

## POLICY

### 1. COLLECTION OF PERSONAL INFORMATION

We collect personal information:

- a. where collection is authorized under a statute, which may include the *Community Charter*, or is authorized under City bylaws;
- b. for the purposes of our activities, services and programs;
- c. for the purposes of planning or evaluating our activities, services and programs;
- d. for law enforcement purposes, including enforcing our bylaws; and
- e. at presentations, ceremonies, performances, sports meets, or similar events, that are open to the public and where you voluntarily appear.

We collect your personal information directly from you, but we may also collect it from another source if you have consented to our doing so. We may collect your personal information from another source in these cases:

- f. where another law allows us to do so;
- g. for law enforcement, for a court proceeding, to collect a debt or fine from you, or to make a payment to you;
- h. where your personal information is necessary for us to deliver, or evaluate, a common or integrated program or activity;
- i. where your personal information is necessary to establish, manage or terminate an employment relationship between you and us;
- j. if your personal information may be disclosed to the City under Part 3 of the Act; or
- k. where we collect your personal information for the purpose of determining your suitability for an honour or award.

### 2. CONSENT, USE AND DISCLOSURE OF PERSONAL INFORMATION

We will use and disclose your personal information only for the purpose we collected it for or for a purpose that is consistent with why we collected it in the first place. We may also use or

disclose your personal information for another purpose if you have identified the information and consented to our other use. Lastly, we may use your personal information for a purpose for which it can be disclosed to us under Part 3 of the Act.

We may also disclose your personal information:

- a. if you have identified the information and consented in writing to its disclosure;
- b. to our employees or service providers if the information is necessary for their duties, for delivery of a common or integrated program or activity, or for planning or evaluating a City program or activity;
- c. if your personal information is made publicly available in British Columbia by a law that authorizes or requires it to be made public;
- d. to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding;
- e. to your union representative who is making an inquiry, if you have given the representative written authority to make the inquiry or it is otherwise authorized;
- f. to our legal counsel for the purpose of legal advice or for use in legal proceedings involving us;
- g. to your Member of the Legislative Assembly if you have asked her or him to help resolve a problem; or
- h. as otherwise permitted under Part 3 of the Act.

Please note that all information provided at open meetings of Council or its committees is considered to be public. If you provide or disclose your personal information to us for that purpose, you are consenting to that information being available to the public, including through posting on our website. This information is considered to be a part of the public record and cannot be removed or changed. However, if you satisfy us in advance that you have legitimate personal safety concerns for yourself or an immediate family member, we may allow you to submit your personal information to Council or a committee in confidence. We will not make it publicly available in that case, although we will keep it in our Legislative Services office, as part of the record.

Express consent is always required when personal information is considered sensitive. Consent can be obtained in a variety of ways, including but not limited to: in person, by mail, by phone, and via the internet. Consent clauses should be easy to find and use clear and straightforward language. Records are to be kept of the consent received such as by notes to file, copy of email, copy of check-off boxes, and signature next to statement on forms. If you wish to withdraw consent at any time, please contact the Legislative Services department.

### **3. ACCURACY OF PERSONAL INFORMATION**

We make every reasonable effort to ensure that personal information we use to make a decision directly affecting you is accurate and complete.

#### **4. ACCESS TO PERSONAL INFORMATION**

You can ask us to give you a copy of your personal information that is in our custody or control by contacting the Legislative Services department. If you are an employee and would like a copy of your own employee personal information, you will need to contact the Human Resources department.

If we believe your request may involve someone else's personal information, or information protected under the Act, we may require you to make a formal request under the Act for access to records. The Act gives us 30 business days to respond to a formal request, starting on the date your request is received (the Act also allows that time to be extended). Please note that in some cases the Act may require us to refuse you access to even your own personal information. We will give you written reasons for every decision on a formal request.

Before disclosing your personal information, we will require you to verify your identity, so we can be assured that you are the individual whose information is being requested. This helps ensure we do not disclose your personal information to someone we should not give it to.

#### **5. CORRECTION OF PERSONAL INFORMATION**

If you believe there is an error or omission in your personal information that we have, you can contact us in writing and ask us to correct it. If we are satisfied that your request is reasonable, we will correct your information as soon as reasonably possible. If we decide not to correct your information, we will note your requested change on the information as well as why we did not correct your information as you asked. This paragraph applies only to factual errors or omissions of your personal information that is in our custody, not opinions or evaluations about you.

#### **6. RETENTION AND DISPOSAL OF PERSONAL INFORMATION**

If we use your personal information to make a decision that directly affects you, we will keep it for at least one year after we make our decision. We also keep personal information in accordance with our relevant record retention schedules. We use reasonable efforts to ensure that your personal information is destroyed securely when the time comes under our records retention schedules.

#### **7. RESPONSIBLE USE OF INFORMATION AND INFORMATION TECHNOLOGY**

Your privacy matters to us, so we use what we believe are reasonable security arrangements to protect your personal information against such risks as unauthorized access, collection, use and disclosure. These arrangements may include information technology measures, as well as policies and practices, to protect your personal information.

If we disclose your personal information to our service provider, we will make reasonable efforts to impose contractual protections on the service provider. Those protections vary according to the nature and sensitivity of the personal information involved. We require our service providers not to use or disclose personal information other than for the purpose of performing services for us.

All employees are required to respect the confidentiality of personal information they receive or compile and are required to use and disclose it only in accordance with this policy and the Act.

## **8. RESPONDING TO PRIVACY-RELATED COMPLAINTS**

Any complaint about any privacy-related matter under this policy or under the Act must be made to us in writing.

We will consider your complaint, including about a breach of your privacy, and will disclose the outcome to you in writing. We expect you to co-operate reasonably and in a timely way with our work, including by promptly providing us with information that we might reasonably need to do our work.

You can seek advice or information from the Office of the Information and Privacy Commissioner for British Columbia. You can also make a written formal complaint to that Office, although we encourage you to use our complaint procedure first. Wherever we can, we try to work things out directly with people, to their satisfaction.

## **9. EDUCATION AND AWARENESS**

All City employees require training on *FIPPA* and privacy generally as appropriate to their work function. Additional training is required in the following circumstances:

- Employees handling high-risk or sensitive personal information electronically require training related to information systems and their security, in co-ordination with the IT department's training.
- Employees managing programs or activities require training related to privacy impact assessments.
- Employees managing common or integrated programs or activities require training related to information sharing agreements.

## **10. PRIVACY RISK ASSESSMENT**

Privacy impact assessments (PIAs) are conducted to determine if a current or proposed system, project, program or activity meets or will meet the requirements of Part 3 of *FIPPA*. A PIA will be done for all new projects involving personal information and for any new collection, use or disclosure of personal information. It will also be conducted for common or integrated programs or activities and data-linking initiatives as well as when significant modifications are made to existing systems, programs or activities.

## **11. PRIVACY BREACH MANAGEMENT & PROTOCOLS**

Information regarding our procedure for responding to a privacy breach is outlined in the document RM-05 Privacy and Information Security policy.

## **12. SERVICE PROVIDER MANAGEMENT**

Employees who prepare or manage contracts are to include the privacy protection schedule or standard privacy language, as designated by the Privacy Officer, in all contracts that involve the service provider having access to, or collecting, using or disclosing, personal information in the custody or under the control of the City.

### 13. EXTERNAL COMMUNICATIONS

We will contact an individual in the following circumstances:

- To give notice of collection of their personal information
- When individuals request access to their personal information or access to records where someone else's personal information is involved
- When responding to requests for correction of personal information
- When personal information is disclosed without consent for compelling health or safety reasons
- When the City intends to give access to personal information in response to a freedom of information request.

### 14. ROLES & RESPONSIBILITIES

#### **Chief Administrative Officer**

- Approves policy and procedures and ensures all employees are given notice of, and access to, a copy of the policy.

#### **Department Heads**

- Support and co-operate with the Privacy Coordinator in implementing the policy and in complying with *FIPPA*.

#### **Corporate Officer/FOI Head**

- Responsible for overseeing the duties and responsibilities of the Records/Information & Privacy Coordinator

#### **Records/Information & Privacy Coordinator**

- Under the direction of the FOI Head, responsible for the development, management and implementation of the City's privacy management program including ongoing assessments and revisions.
- Coordinates employee training and education, ensuring that all new employees receive *FIPPA* orientation and training within the first year of their employment.

*See RM-02 Records Management Accountability Policy for full listing of roles and responsibilities with respect to management and governance of information and records.*

### CONTACT INFORMATION

If you have any questions about this policy or your personal information please contact Legislative Services at (250) 755-4405 or by email at [foi@nanaimo.ca](mailto:foi@nanaimo.ca)

### AUTHORITY TO ACT

The Corporate Officer is delegated responsibility and authority for ensuring compliance with this policy and *FIPPA*.

## RELATED DOCUMENTATION

### Legislation

City of Nanaimo's Freedom of Information and Protection of Privacy Bylaw 2006 No. 7024  
*Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165)

### Records Management Policies and Procedures

RM-01 Records Management Framework Policy  
RM-02 Records Management Accountability Policy  
RM-03 Records Management Policy  
RM-04 Legal Hold Policy  
RM-06 Scanning and Imaging Policy  
RM-07 Email Management Policy  
RM-08 Vital Records and Business Continuity Policy  
RM-09 Access to Information Policy  
RM-10 Mobile Device Policy  
RM-11 Records in the Custody of Council Policy

## POLICY REVIEW

This policy shall be reviewed by the Corporate Records Officer at least every 3 years.

Date: 201X-XXX-XX Approved by: