City of Grand Forks
7217 4th Street
Grand Forks, BC V0H 1H0
250.442.8266
www.grandforks.ca

Council Policy

Privacy Policy

Approval Date: March 6, 2023
Resolution No.: R063/23/03/06
Rescinded: N/A

Contact Department: Corporate Services

Purpose

The purpose of the City of Grand Forks' Privacy Policy is to describe how the City collects, uses, discloses, and protects *Personal Information*.

Intent

This policy provides a framework for how the City will operate 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*).

Statutory Provisions

This policy is established in accordance with the City's "*Freedom of Information and Protection of Privacy Bylaw 2047*" and the Province of British Columbia's "*Freedom of Information and Protection of Privacy Act*", both as amended or replaced from time to time.

Definitions

In this policy, the following meanings apply:

"Act"	means the *Freedom of Information and Protection of Privacy Act (British Columbia)* as may be amended or replaced from time to time;
"Commissioner"	means the Information and Privacy Commissioner for the Province of British Columbia;
"City"	means the City of Grand Forks;
"Employee"	means an employee of the *City*, including a volunteer or service provider;
"Personal Information"	means recorded information about an identifiable individual (but does not include information to enable an individual at a place of business to be contacted, such as the name, position name or title, business telephone number, business address, business email or business fax number of the individual);
"Privacy Officer"	means the Corporate Officer or delegate who is responsible for being the primary contact for privacy-related matters and supporting the *City*'s compliance with the *Act*.
"Service Provider"	means a person or organization retained under a contract to perform services for the *City*;

Interpretation

In this policy, a reference to a person who holds an office includes a reference to the persons appointed as deputy to, or appointed to act for, that person from time to time.

Policy Statements

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.

1. Collection of Personal Information

1.1. The *City* may collect *Personal Information*:

1.1.1 where collection is authorized under a statute, such as the *Community Charter* (British Columbia) and the *Local Government Act* (British Columbia), or is authorized under *City* bylaws;

1.1.2 for the purposes of *City* activities, services, and programs;

1.1.3 for the purposes of planning or evaluating *City* activities, services, and programs;

1.1.4 for law enforcement purposes, including enforcing the *City's* bylaws; and

1.1.5 at presentations, ceremonies, performances, sports meets, or similar events, that are open to the public and where individuals voluntarily appear, such as public meetings and public hearings.

1.2. *The City* collects *Personal Information* directly from individuals but may also collect information from another source if an individual has consented to the *City* doing so. The City may also collect *Personal Information* from another source as permitted under the *Act*, including in these cases:

1.2.1 where another law allows *The City* to do so;

1.2.2 for law enforcement, for a court proceeding, to collect a debt or fine, or to make a payment;

1.2.3 where *Personal Information* is necessary for the *City* to deliver, or evaluate, a common or integrated program or activity;

1.2.4 where *Personal Information* is necessary to establish, manage or terminate an employment relationship between the *City* and an individual;

1.2.5 if *Personal Information* may be disclosed to the *City* under Part 3 of the Act; or

1.2.6 where the *City* collects *Personal Information* for the purpose of determining a person's suitability for an honour or award.

1.3. *The City* will endeavour to limit the amount of *Personal Information* recorded to that which is necessary to fulfill the purpose for which the information is being collected.

2. Use and Disclosure of Personal Information

2.1. The *City* will use and disclose *Personal Information* only for the purpose the *City* collected it for or for a purpose that is consistent with why the *City* collected it in the first place.

2.2. The *City* may also use or disclose *Personal Information* for another purpose if an individual has identified the information and consented to the *City's* other use.

2.3. The *City* may use *Personal Information* for a purpose for which the information can be disclosed to the *City* under Part 3 of the *Act*.

2.4. The *City* may also disclose a person's *Personal Information*:

2.4.1 if the person has identified the information and consented in writing to its disclosure;
2.4.2 to the *City*'s *Employees* 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;
2.4.3 if the *Personal Information* is made publicly available in British Columbia by a law that authorizes or requires it to be made public;
2.4.4 to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding;
2.4.5 to a person's union representative who is making an inquiry, if the person has given the representative written authority to make the inquiry, or it is otherwise authorized;
2.4.6 to the *City's* legal counsel for the purpose of legal advice or for use in legal proceedings involving the *City*;
2.4.7 to an person's Member of the Legislative Assembly if the person have asked her or him to help resolve a problem; or
2.4.8 as otherwise permitted or required under Part 3 of the *Act*.

2.5. Please note that all information provided at open meetings of Council or its committees is considered to be public. If a person provides or discloses their *Personal Information* to the *City* for that purpose, the person is consenting to that information being available to the public, including through posting on *the City's* website or webcasting. This information is considered to be a part of the public record and cannot be removed or changed. However, if a person satisfies the *City* in advance that the person has legitimate personal safety concerns for themselves or an immediate family member, the *City* may allow the person to submit their *Personal Information* to Council or a committee in confidence. The *City* will not make the *Personal Information* publicly available in that case, although the *City* will keep it in the Corporate Services office, as part of the record.

3. Accuracy of Personal Information

3.1. The *City* will make every reasonable effort to ensure that *Personal Information* the *City* uses to make a decision directly affecting a person is accurate and complete.

4. Access to Personal Information

4.1. A person can ask the *City* to give them a copy of their *Personal Information* that is in the City's custody or control by contacting the Corporate Services department.

4.2. If an *Employee* of the *City* would like a copy of their own employee *Personal Information*, the *Employee* will need to contact the Corporate Services department.

4.3. If the *City* believes a person's request may involve someone else's *Personal Information*, or information protected under the *Act*, the *City* may require the person to make a formal request under the *Act* for access to those records. The *Act* defines the amount of time the *City has* to respond to a formal request (presently 30 business days), starting on the date a request is received (the *Act* also allows that time to be extended). In some cases the *Act* may require the *City* to refuse access to even a person's own *Personal Information*. The *City* will give the requestor written reasons for every decision on a

formal request.

4.4. Before disclosing a person's *Personal Information*, the *City* will require the person to verify their identity, so the *City* can be assured that the requestor is the individual whose information is being requested. This helps ensure that the *City* does not disclose a person's *Personal Information* to someone to whom it should not be given.

5. Correction of Personal Information

5.1. If a person believes there is an error or omission in or from their *Personal Information*, the person can contact the *City* in writing and ask the *City* to correct it. If the *City* decides to correct that information, the *City* will do so as soon as reasonably possible. If the *City* decides not to correct the information, the *City* will note the requested change on the information as well as why the *City* did not correct the information as requested.

6. Retention and Disposal of Personal Information

6.1. If the *City* uses *Personal Information* to make a decision that directly affects a person, the *City* will keep the information for at least one year after the *City* makes the decision. *The City* shall also keep *Personal Information* in accordance with *the City's* relevant record retention schedules. The *City* will use reasonable efforts to ensure that *Personal Information* is destroyed securely when the time comes under the *City's* records retention schedules.

7. Responsible Use of Information and Information Technology

7.1. Individuals privacy matters to the *City*, so the *City* will use what the *City* believes are reasonable security arrangements to protect a person's *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 a person's *Personal Information*.

7.2. If the *City* discloses a person's *Personal Information* to one of the *City's* service providers, the *City* 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. The *City* requires *the City's* service providers not to use or disclose *Personal Information* other than for the purpose of performing services for the *City*.

7.3. All *City 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

8.1. The procedure for registering a privacy complaint with the *City* are outlined in section 1 of Appendix A attached to this policy.

9. Education and Awareness

9.1. All *City Employees* receive training on the *Act* and privacy generally as appropriate to their work function. Additional training is given in the following circumstances:

9.1.1 *Employees* handling what the *City* considers high-risk or sensitive *Personal Information* electronically receive training related to information systems and their security, in co- ordination with the IT department's training;

9.1.2 *Employees* managing programs or activities receive training related to privacy impact assessments; and

9.1.3 *Employees* managing common or integrated programs or activities receive training related to information sharing agreements.

10. Privacy Impact (Risk) Assessments

10.1. Privacy impact assessments (PIAs) are conducted to determine if a proposed system, project, program, or activity meets or will meet the requirements of Part 3 of the *Act*.

10.2. A PIA will be done for any new system, project, program, or activity involving *Personal Information* and for any new collection, use or disclosure of *Personal Information*.

10.3. A PIA 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, projects, programs, or activities.

11. Privacy Breach Management and Protocols

11.1. The procedures for responding to a privacy breach are outlined in Appendix A of this policy.

12. Service Provider Management

12.1. *Employees* who prepare or manage contracts with service providers shall include the privacy protection schedule or standard privacy language, as designated by the Corporate 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

13.1. Under this policy, the *City* will contact an individual in the following circumstances:

13.1.1 To give notice of collection of their *Personal Information*;

13.1.2 When individuals request access to their *Personal Information* or access to records where someone else's *Personal Information* is involved;

13.1.3 When responding to requests for correction of *Personal Information*;

13.1.4 When *Personal Information* is disclosed without consent for compelling health or safety reasons; and

13.1.5 When the *City* intends to give access to *Personal Information* in response to a freedom of information request.

14. Roles and Responsibilities

14.1. Chief Administrative Officer

14.1.1 Approves administrative policies and procedures and ensures all *Employees* are given notice of, and access to, a copy of the policy.

14.2. Department Heads

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

14.3. Corporate Officer/FOI Head

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

14.4. Records, Information, and Privacy Coordinator

14.4.1 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.

14.4.2 Coordinates employee training and education, ensuring that all new employees receive orientation and training regarding the *Act* within the first year of their employment.

15. Authority To Act

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

16. Review

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

Resolutions and Amendments

APPENDIX A: Procedures for Managing Privacy Breaches

1. Privacy Complaints and Breaches

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

1.2. The *City* will consider a person's complaint, including about a breach of your privacy, and will disclose the outcome to the person in writing. The *City* expects a complainant to co-operate reasonably and in a timely way with the *City's* work, including by promptly providing the *City* with information that the *City* might reasonably need to do the *City's* work. A complainant's failure to do so may result in the *City's* deciding not to proceed any further with the complaint.

1.3. A person may make a written formal complaint to the Office of the Information and Privacy Commissioner for British Columbia, although the *City* encourages individuals to use *the City's* complaint procedure first. Wherever the *City* can, the *City* will endeavour to work things out directly with people to their satisfaction.

2. Required to Notify

2.1. Upon notice of a privacy break, the privacy officer shall be contacted, in writing, without unreasonable delay.

2.2. The privacy head shall, without unreasonable delay,:

2.2.1 notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including:

- 2.2.1.1. identity theft or significant bodily harm,
- 2.2.1.2. humiliation,
- 2.2.1.3. damage to reputation or relationships,
- 2.2.1.4. loss of employment, business or professional opportunities,
- 2.2.1.5. financial loss,
- 2.2.1.6. negative impact on a credit record, or
- 2.2.1.7. damage to, or loss of, property

2.2.2 notify the commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph 2.2.1 above.

3. Notification Procedures

3.1. Direct Notification for Affected Individuals

3.1.1 Notifications must include the following information:

- 3.1.1.1. the name of the public body;
- 3.1.1.2. (the date on which the privacy breach came to the attention of the public body;
- 3.1.1.3. a description of the privacy breach including, if known,
- 3.1.1.4. the date on which or the period during which the privacy breach occurred, and
- 3.1.1.5. a description of the nature of the *Personal Information* involved in the privacy breach;
- 3.1.1.6. confirmation that the commissioner has been or will be notified of the privacy breach (per section 2.2.2 of this appendix);
- 3.1.1.7. contact information for a person who can answer, on behalf of the

public body, questions about the privacy breach;

3.1.1.8. a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;

3.1.1.9. a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

3.2. Indirect Notifications for Affected Individuals

3.2.1 A notification may be given to an affected individual in an indirect manner if

3.2.1.1. the public body does not have accurate contact information for the affected individual,

3.2.1.2. the head of the public body reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the public body, or

3.2.1.3. the head of the public body reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner.

3.2.2 If a notification must be given in an indirect manner, the notification must

3.2.2.1. be given by public communication that can reasonably be expected to reach the affected individual, and

3.2.2.2. contain the following information:

a. the name of the public body;
b. (the date on which the privacy breach came to the attention of the public body;
c. a description of the privacy breach including, if known,
   (i) the date on which or the period during which the privacy breach occurred, and
   (ii) a description of the nature of the *Personal Information* involved in the privacy breach;
d. confirmation that the commissioner has been or will be notified of the privacy breach;
e. contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
f. a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
g. a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

3.3. Notifications to the Commissioner

3.3.1 A notification to the Commissioner under section 36.3 (2)(b) of the *Act* must be given to the commissioner in writing and must include the following information:

3.3.1.1. the name of the public body;

3.3.1.2. the date on which the privacy breach came to the attention of the public body;

3.3.1.3. a description of the privacy breach including, if known,

a. the date on which or the period during which the privacy breach occurred,
b. a description of the nature of the *Personal Information* involved in the privacy breach, and
c. an estimate of the number of affected individuals;

3.3.1.4. contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

3.3.1.5. a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

3.4. Not Required to Notify

3.4.1 Per section 36.3(3) of the *Act*, "[t]he head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to

3.4.1.1. result in immediate and grave harm to the individual's safety or physical or mental health, or

3.4.1.2. threaten another individual's safety or physical or mental health."

3.5. Disregarding Requests

3.5.1 If the privacy head asks, the commissioner may authorize the public body to disregard a request if:

3.5.1.1. a request is frivolous or vexatious,

3.5.1.2. a request is for a record that has been disclosed to the applicant or that is accessible by the applicant from another source, or

3.5.1.3. responding to the request would unreasonably interfere with the operations of the public body because the request

a. is excessively broad, or
b. is repetitious or systematic.