



PRIVACY MANAGEMENT PROGRAM POLICY

Department	Corporate Administration	Policy No.	0340-96
Section		Date Approved by Board	August 14, 2025
Repeals		Board Resolution #	RD/25/08/47

Amended		Board Resolution #	
Amended		Board Resolution #	
Amended		Board Resolution #	

Repealed		Board Resolution #	
----------	--	--------------------	--

1. PURPOSE

The purpose of the Peace River Regional District (PRRD) Privacy Management Program Policy is to describe how the PRRD collects, uses, discloses and protects Personal Information. This policy provides a framework for how the PRRD will operate in order to ensure Personal Information is managed in accordance with the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

2. SCOPE

This policy applies to all PRRD employees, Board members, Committee and Commission members, other volunteers, and contracted service providers while performing their duties under contract to the PRRD.

The privacy obligations of the PRRD equally apply and flow down to all service providers where collection, use, disclosure, security and access to personal information may be required while performing services under contract to the PRRD.

3. DEFINITIONS

Act means the *Freedom of Information and Protection of Privacy Act* RSBC 1996 c. 165, as amended;

Contact Information means information that would enable an individual to be contacted at a place of business and includes: name, position or title, business telephone number, email address and fax number as well as business address.

FOIPPA Head means the person designated by the PRRD Board in accordance with FOIPPA as a statutory decision maker for the purpose of administering and complying with FOIPPA in the organization. The FOIPPA Head is typically also designated at the PRRD Privacy Officer who as administrative oversight of the PRRD Privacy Management Program.

Information Sharing Agreements (ISA) means a process when there is regular and systematic exchange of Personal Information between public bodies, OR between public bodies and external agencies. An ISA sets out the terms and conditions of the exchange of Personal Information in compliance with the provisions of FOIPPA and any other applicable legislation.



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)

Service Provider means a person retained under contract to perform services for the Peace River Regional District.

4. **POLICY**

This policy is established in accordance with the PRRD Freedom of Information and Protection of Privacy Administration Bylaw and in accordance with the Act.

Roles and Responsibilities

1. Chief Administrative Officer approves policy and procedures and ensures all employees are given notice of and access to a copy of this policy and relevant procedures.
2. Department Heads support and cooperate with the Corporate Officer/FOI Head in implementing the policy and in complying with the Act
3. Corporate Officer/FOI Head is responsible for overseeing the development, management and implementation of the PRRD's Privacy Management Program including ongoing assessments and revisions, and privacy related training and awareness among staff.
4. PRRD employees, Board Members, Committee and Commission members and other volunteers are responsible for reading and understanding this policy, following the PRRD's individual privacy policies and protocols and contacting the Corporate Officer with any access or privacy questions when necessary.
5. Service Providers are responsible for understanding their responsibilities to protect personal information as described within this policy.

Authority to Act

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

Collection of Personal Information

7. The PRRD collects information:
 - a. As authorized by statute (e.g. *Community Charter* and the *Local Government Act*);
 - b. For the purposes of PRRD activities, services and programs;
 - c. To verify identity;
 - d. For the purposes of planning or evaluating activities, services and programs;
 - e. For law enforcement purposes, including enforcement of PRRD Bylaws; and
 - f. At events that are open to the public where people voluntarily appear, such as public meetings and public hearings.

Use and Disclosure of Personal Information

8. The PRRD will use and disclose personal information only for the purpose it was collected for, or for a purpose consistent with why it was collected in the first place.
9. The PRRD may also use or disclose personal information for another purpose if the person has identified the information and has consented in the prescribed manner to the disclosure.



10. In addition, the PRRD may also disclose personal information:
 - a. to PRRD employees or service providers if the information is necessary for their duties, for delivery of a program or activity or for planning or evaluating a PRRD program or activity;
 - b. if the personal information is made publicly available in British Columbia by a law that authorizes or requires it to be made public;
 - c. to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding;
 - d. to PRRD's legal counsel for the purpose of legal advice or for use in legal proceedings;
 - e. as otherwise permitted or required under [Part 3 of the Act](#).
11. All information provided at open meetings of the Board, or its Committees is considered to be public. If personal information is provided or disclosed for that purpose, consent is understood to be given to that information being available to the public, including posting on our website and videorecording and the livestream on the PRRD's social media. This information is considered to be a part of the public record and cannot be removed or changed. However, if an individual can satisfy the PRRD they have legitimate personal safety concerns for themselves or an immediate family member, the PRRD may allow personal information to be submitted to the Board or its Committees in confidence and, in that case, will not make it publicly available although it will be kept in the Corporate Administration office as part of the record for that meeting.

Accuracy of Personal Information

12. The PRRD will make every reasonable effort to ensure that personal information used to make a decision directly impacting that person is accurate and complete.
13. A request to provide a copy of personal information provided to the PRRD which is now under the PRRD's custody or control can be made by contacting the Corporate Administration department. All PRRD employees need to contact Human Resources if a copy of employee personal information is requested.
14. If the PRRD has reason to believe a request for personal information may involve someone else's personal information or information protected under the Act, the PRRD may require a formal request under the Act for Access to Records. The Act gives the PRRD 30 business days to respond to a formal request starting on the date the request is received and allows that time to be extended. In some cases the Act may require the PRRD to refuse access and the PRRD will provide written reasons for every decision on a formal request.
15. Before disclosing personal information, the PRRD will require verification of identity. This helps ensure the PRRD does not disclose personal information to an unauthorized person.

Correction of Personal Information

16. In the instance it is believed that an error or omission in or from personal information has occurred, contact the PRRD in writing to request that the personal information is corrected. The PRRD will correct the information as soon as reasonably practicable if the PRRD deems the information does in fact require correction. If the PRRD decides not to correct the information, the requested change and reason why it was not corrected will be noted on the information.

Retention and Disposal of Personal Information

17. The PRRD utilizes records retention policies customized for each area of the organization that take into account the length of time information must be retained. If an individual's personal information is used to make a decision, a record of that decision will be kept for a minimum of



one year after the decision has been made. Once personal information is no longer needed, it is authorized for destruction and is confidentially disposed of.

Responsible Use of Information and Information Technology

18. The Regional District uses every reasonable security arrangement to protect personal information against such risks as unauthorized access collection, use and disclosure. These arrangements may include information technology measures, as well as policies and procedures to protect personal information.
19. Should the PRRD disclose personal information to its service providers, reasonable efforts to impose contractual protections on the service provider will be made. Those protections vary according to the nature and sensitivity of the personal information.
20. All PRRD 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.
21. The PRRD website automatically collects and stores the following information from visitors to the website:
 - a. The internet protocol (IP) address and domain name used (the IP address is a numerical identifier assigned to either the individual's internet service provider or directly to the computer);
 - b. The type of browser and operating system;
 - c. The date and time of the visit;
 - d. The webpage(s) accessed; and
 - e. Amount of time spent on each page.
22. Information automatically collected is used only for the purposes of administering the website, assessing system performance, improving services and website management. The Regional District will not use this data to determine the inquirer's identity unless required to do so as part of an internal investigation for law enforcement purposes.
23. Personal information such as names, email addresses and demographic information is only obtained when individuals supply it voluntarily through contacting us via email or using the forms available on our website. This information will only be used for statistical purposes and/or to support the person's relationship with the PRRD.
24. The PRRD's website may include links to webpages operated by other organizations. These links are not intended to be referrals and are posted only for convenience. The PRRD has no responsibility for, liability, or control over these links or websites. Please refer to the individual privacy policies and terms and conditions of use for all external websites.

Privacy Complaints and Breaches

25. A privacy breach is the theft or loss of personal information, or the access, collection, use or disclosure of personal information in the custody or control of a public body that is not authorized by the Act. A privacy complaint is a complaint from an individual about a breach of their own personal information.
26. All employees have a duty to report suspected privacy breaches (accidental or intentional) to their supervisor or department head, or to the Corporate Officer directly.
27. As outlined in the Act, if a privacy breach is reasonably expected to result in significant harm to an individual, the PRRD is required to issue a notification about that breach to the affected individual and to the Information and Privacy Commissioner.



28. Any complaint about any privacy related matter under this policy or under the Act must be made to the PRRD in writing. The PRRD will consider the complaint including about a breach of privacy and will disclose the outcome of the complaint in writing. The PRRD expects the complainant to cooperate reasonably and in a timely way with the PRRD's work, including promptly providing information that the PRRD may reasonably need to complete the work. Failure to cooperate reasonably may result in a decision not to proceed any further with the complaint.
29. A formal complaint may be made to the Office of the Information and Privacy Commissioner for British Columbia, although it is preferred to use the PRRD complaint procedure first and, wherever possible, the PRRD will try to work things out directly to the satisfaction of the complainant.

Privacy Awareness and Education Activities

30. All PRRD employees receive training on the Act and on privacy generally as appropriate to their work function. Additional training is provided in the following circumstances:
 - a. Employees handling what the PRRD considers high-risk or sensitive personal information electronically receive training related to information systems and their security;
 - b. Employees managing programs or activities, receive training related to Privacy Impact Assessments; and
 - c. Employees managing common or integrated programs or activities receive training related to Information Sharing Agreements.

Privacy Impact Assessments

31. Privacy Impact Assessments (PIAs) are conducted to determine if a proposed system, project, program or activity meets or will meet the privacy requirements of the Act and mitigate privacy risks. A PIA will be completed for any new system, project, program or activity involving personal information and for any new collection, use or disclosure of personal information. A PIA will also be conducted for common or integrated programs or activities and data-linking initiatives, as well as when significant modification are made to existing systems, projects, programs or activities.

Information Sharing Agreements

32. If initiatives include regular systemic exchange of personal information with partners outside of the public body, an Information Sharing Agreement must be completed and submitted to the Corporate Officer.

Service Provider Management

33. Employees who prepare or manage contracts with service providers are to include the 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 PRRD.

Monitoring and Updating

34. This policy shall be reviewed by the Corporate Officer at least every three years.

Contact Information

35. For questions about this policy or use of personal information, contact the PRRD's Corporate Officer.



Affiliated Policies	
Affiliated Procedure	<ul style="list-style-type: none">• PRRD Template for Privacy Impact Assessments must be used• PRRD Template for Information Sharing Agreement must be used