Policy Title: Information Access & Privacy Protection	Policy Number: P95
Policy Category: Administration	
Approval Date: February 28, 2023	**Policy Owner:** Corporate Services
Approved by: CVRD Board	**File Reference:** 0340-50

PREAMBLE

1. The Comox Valley Regional District (CVRD) is subject to the *Freedom of Information and Protection of Privacy Act* ("Act") and is committed to the responsible management of personal and confidential information within the CVRD's custody and/or control.

   The Act was proclaimed in 1993 and provides for information access and privacy rights in British Columbia. The purpose of the legislation is to provide the public with the right to request access to the records of public bodies, including a right of access to and a right to request correction of personal information about themselves. The Act also provides for a list of exceptions to the right of access, to balance the right of access with a need for confidentiality. The Act prevents the unauthorized collection, use or disclosure of personal information by public bodies and provides for an independent review of all CVRD decisions made under the Act by the Office of the Information and Privacy Commissioner (OIPC).

PURPOSE

2. This policy establishes the CVRD's privacy obligations for the collection, use, disclosure, access, storage, retention, and disposal of Personal Information, as required by the Act, other legislation and fair information management practices.

SCOPE

3. This policy applies to all CVRD employees, elected officials, volunteers, and contracted service providers while performing their duties under contract to the CVRD.

   The privacy obligations of the CVRD 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 CVRD.

DEFINITIONS

4. In this policy,
   "Act" means the *Freedom of Information & Protection of Privacy Act*;

   "Applicant" means a person who submits a request for access to CVRD records in accordance with the Act;

   "Confidential Information" means a category of information with strict confidentiality requirements including but not limited to:

i. economic or financial information;
ii. third party business information, where its disclosure could harm the third party;
iii. legal advice;
iv. law enforcement information;
v. the substance of deliberations of an In-Camera meeting; and
vi. other proprietary information of the CVRD;

"Contact Information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

"Control" is the power or authority to manage a record throughout its life cycle;

"Custody" means having physical possession of a record, including responsibility for access, managing, maintaining, preserving, disposing, and providing security;

"FOI request" means a Freedom of Information request for access to records pursuant to section 5 of the Act;

"Coordinator" The Manager of Corporate Records and Information or, in the absence of the Manager of Corporate Records and Information the Corporate Legislative Officer or deputy, is designated as the Coordinator for the purposes of the Act

"Personal information" means recorded information about an identifiable individual other than business contact information;

"Privacy Impact Assessment (PIA)" A privacy impact assessment identifies and mitigates the risks to personal information arising from the implementation of new projects and assists with compliance to the Act.

"Head" means the Corporate Legislative Officer or deputy, who is designated as the Head as per the Act and as appointed by the Board by bylaw;

"Record" includes books, documents, maps, drawings, letters, papers, and any other mechanism on which information is recorded or stored by mechanical, graphic, electronic, or other means;

"CVRD" means the Comox Valley Regional District;

"Responsive Record" means a record that fits within the scope of an FOI request.

POLICY

6.1 Protection of Personal Information

6.1.1 The CVRD will observe and ensure the following standards established by the Act regarding the collection, use, disclosure, and security of personal information:

(a) Personal information within the CVRD's custody and/or control will be protected at all times;

(b) Personal information will only be collected if the collection is authorized by legislation, is necessary for law enforcement, or is necessary for the operation of a program or activity of the CVRD;

(c) Whenever possible, personal information will be collected directly from the individual the information is about;

(d) If personal information will be collected indirectly, The CVRD will ensure the collection is authorized under the Act;

(e) When collecting personal information, the CVRD will inform the individual of the specific use(s) of their information, the legal authority for the collection of that information, and the contact information of someone in the organization who can answer their questions about the collection;

(f) When collecting personal information from citizens who call the CVRD, employees must advise the citizen what their personal information will be used for, that the personal information may be retained for future communications with the citizen, and that the citizen may contact the Head if they have any questions regarding the collection, use or disclosure of their personal information;

(g) The CVRD will include a *Notice of Collection* on all CVRD forms used to collect personal information;

(h) The CVRD will only use personal information for the purpose for which it was collected or for a purpose consistent with that initial purpose, meaning the use has a reasonable and direct connection to the original stated purpose;

(i) Permitting storage or access of sensitive personal information outside of Canada will be a risk-based decision determined through the completion of a Privacy Impact Assessment.

6.1.2 CVRD employees must attend privacy training provided by the CVRD through orientation or onboarding processes as applicable. Periodic refresher training must also be attended to ensure knowledge on privacy processes and practices.

6.1.3 All CVRD employees and volunteers will read and sign the applicable staff and volunteer code of conduct to ensure they understand their role and responsibilities in the protection of personal information under the custody and/or control of the CVRD.

6.1.4 A Personal Information Bank, which is a record of the types and sensitivities of personal information being held by each department, will be maintained by the head. This enables the CVRD to ensure all personal information in its custody and/or control is properly secured and protected from inappropriate use or disclosure.

6.1.5 CVRD employees and elected and appointed officials, where applicable, will use their assigned corporate email accounts when conducting CVRD business, including when working remotely. Personal email accounts must never be used to conduct CVRD business. CVRD employees will follow all applicable policies and procedures to ensure that:

(a) the CVRD is compliant with the Act;

(b) corporate email is being used appropriately; and

(c) unnecessary business risks to the CVRD by misuse of corporate email is avoided.

6.1.6 When travelling with personal/confidential information or working offsite at another location, CVRD employees and elected and appointed officials will take measures to protect electronic and paper records, especially those containing personal or confidential information, from risks such as unauthorized collection, use, disclosure, access, and destruction.

6.1.7 Where disclosures of personal information are occurring on a regular basis with an external third party, an Information Sharing Agreement (ISA) will be developed to document the expectations of the CVRD and the third party regarding the security and protection of the personal information being disclosed or exchanged.

6.2 Correction of Personal Information

Under the Act, an individual whose information is in a public body's custody and/or control, and who believes there is an error or omission in their personal information, can make a request to the public body to correct the information. CVRD employees who receive a request from an individual for their personal information to be revised shall contact the Head who will address the request.

6.3. Disclosure of Personal Information to Law Enforcement, Government Bodies, or Emergency Personnel

6.3.1 Under the Act, the CVRD is authorized to disclose personal information to Canadian law enforcement agencies to assist in a law enforcement investigation. Non-emergency requests for personal information will be referred to the Head for response.

6.3.2 In emergency situations, where there is not enough time to refer the matter to the Head, CVRD employees may disclose personal information directly to law enforcement agencies if it is necessary to avert a risk of significant harm to health or safety. There must be a danger to a person's physical or mental health or a threat to a person's life for the disclosure to fall under this provision.

6.3.3 Under the Act, the CVRD may disclose personal information to Canadian government bodies in accordance with an enactment (law) of BC or Canada that authorizes or requires its disclosure. The government body must make the request in writing and must specify the reason for the request and the section of the enactment that authorizes or requires the disclosure.

6.4 Privacy Breaches

6.4.1 A privacy breach occurs when personal information is collected, retained, used, disclosed, accessed, or disposed of in ways that do not comply with the provisions of the Act.

6.4.2 All CVRD employees, including service providers and their employees or associates have a duty to report suspected privacy breaches (accidental or intentional) to the Head directly.

6.4.3 If the privacy breach is reasonably expected to result in significant harm to an individual the CVRD shall notify the affected individual and the Information and Privacy Commissioner.

6.4.4 The CVRD shall maintain a policy providing procedures concerning privacy breaches.

6.5 Privacy Complaints

6.5.1 Individuals have the right under the Act to file a complaint about improper collection, use and/or disclosure of their personal information by the CVRD, or about a decision made by the CVRD concerning a personal information request. Privacy Complaints that are received by the CVRD shall be referred to the Head who will investigate the complaint and remediate as required.

6.6 Privacy Impact Assessments

6.6.1 A Privacy Impact Assessment (PIA) is a mandatory tool for assessing new technologies, programs, processes and enactments involving personal information to ensure the collection, use, disclosure, and/or security of the personal information is compliant with the Act.

6.6.2 Before initiating a new system or process involving personal information, the CVRD will consider whether a PIA is required.

6.6.3 If a PIA is required, the respective department will work with the Coordinator to complete a PIA, using the template established by the Head.

6.7 Video Surveillance

6.7.1 The CVRD may implement video surveillance on CVRD owned or occupied property or buildings where safety or property security matters warrant.

6.7.2 As video surveillance may be considered an unreasonable invasion of personal privacy, the installation of video surveillance equipment will only be considered in unique and exceptional circumstances.

6.7.3 The deployment of video surveillance by the CVRD is not intended to infringe on individuals' rights and is intended only to safeguard CVRD owned assets and the individuals who use those assets.

6.7.4 All video surveillance will be in accordance with established CVRD policy regarding procedures for implementing video surveillance, and guidelines for the access and disclosure of stored video images.

6.8 Online Privacy Statement

6.8.1 The Head will maintain an Online Privacy Statement posted to the CVRDs website, which will provide information to the public on how the CVRD collects, uses, discloses, and secures individuals' personal information.

6.9 Compliance and Auditing

6.9.1 The Head shall periodically review the CVRD's records and systems to ensure the CVRD is in compliance with the Act and that CVRD policies and protocols regarding the management of personal information are being followed.

6.10 Freedom of Information

6.10.1 The Act provides individuals with a right of access to certain records and personal information under the custody or control of the CVRD.

6.10.2 The Head will ensure the CVRD is responsive and accountable to its access obligations under the Act.

6.11 Routine Requests vs FOI Requests

6.11.1 Most requests received by the CVRD are for information that is not sensitive or confidential; these are called routine requests and can be responded to by employees who have access to the respective records.

6.11.2 The CVRD will establish and maintain categories of records that are in the custody or under the control of the CVRD and are available to the public without a formal request for access under the Act.

6.11.3 Requests for records that may contain sensitive or confidential information are called Freedom of Information or FOI requests. These requests are processed by the CVRD in accordance with procedures set out in the Act.

6.12 Duty to Assist

6.12.1 In accordance with the Act, the CVRD will make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately, and completely.

6.12.2 To ensure responses to FOI requests are made within the prescribed timeframe imposed by the Act:

(a) All FOI request shall be forwarded immediately to the Coordinator;

(b) CVRD staff will prioritize and endeavour to provide an acknowledgment response to the Coordinator within five working days to requests for responsive records;

(c) The CVRD will perform a thorough search of all records, including email, for any responsive records;

(e) During retrieval of records, CVRD staff will immediately notify the Coordinator if a large volume of records (100+ pages) is anticipated.

6.12.3 A general framework of the steps required when processing an FOI request under the Act, including roles and responsibilities, is included in Schedule 1.

6.13 FOI Response Process

6.13.1 The Coordinator will respond to all FOI requests in accordance with the Act, including:

(a) Making every reasonable effort to assist applicants;

(b) Responding to requests within prescribed timelines;

(c) Applying exceptions and severing/redacting information as per Division 2 of the Act; and

(d) Providing third party notifications.

6.14 Application of Exceptions

6.14.1 The Coordinator may seek insight and advice from subject matter experts within various departments on issues of particular concern or sensitivity when determining which exceptions to apply to responsive records.

6.15 Executive Management Team (EMT) Updates

6.15.1 The Head will provide regular updates to the EMT on active FOI requests related to potentially sensitive information or with a significant volume of responsive records.

6.16 Office of the Information and Privacy Commissioner

6.16.1 The Coordinator is the main point of contact for the OIPC, an independent body that provides oversight and enforcement of BC's access and privacy laws.

ROLES AND RESPONSIBILITIES

7.1 The Head is responsible for:

a. the development, maintenance, and oversight of the Privacy Program for the CVRD, which establishes the necessary policies and procedures (collectively referred to as the "Privacy Management Program") to ensure the responsible management of information within the CVRD's custody and control;

b. all matters related to the CVRDs' access and privacy obligations under the Act;

c. privacy-related awareness and training;and

d. monitoring program compliance, investigating and tracking privacy incidents and breaches, and ensuring individuals' rights in compliance with privacy law.

7.2.1 The Head shall review this policy and the associated programs and procedures on an annual basis to ensure they remain appropriate to the CVRD's activities and are compliant with the Act.

7.3 The Coordinator is responsible for the following aspects of the Privacy Program:

a. Preparation of responses to, and main point of contact for, FOI requests;

b. Maintenance of records and files related to FOI requests;

c. Compilation of CVRD records in response to FOI requests;

d. Drafting Privacy Breach Reports;

e. Supporting departments when drafting Privacy Impact Assessments;and

f. Other tasks as appointed by the Head.

7.4 CVRD employees, elected and appointed officials, and volunteers are responsible for reading and understanding this Policy, following the CVRD's individual privacy policies and protocols, and contacting the Head with any access or privacy questions whennecessary.

7.5 Service Providers are responsible for understanding their responsibilities to protect personal information and following all such requirements as described within their service agreement with the CVRD.

REVISION HISTORY

11.

Approval Date	Approved By	Description of Change

APPENDIX

APPENDIX 1: FIPPA Process for Managing FOI Requests

Schedule 1
FIPPA Process for Managing FOI Requests

Timeline	Step
Day 1	FOI Request received. If request is received by program area, forward immediately to Information & Privacy Coordinator ("Coordinator").
1-5 business days from date request received	Coordinator prepares and sends acknowledgement letter to applicant.
	Coordinator notifies appropriate program area contact(s) and manager(s) of new request which initiates the search for responsive records. Program area contact(s) retrieve records and respond to Coordinator within five working days. Search must include all hard copy and electronic records.
	During retrieval of records, program area contact must immediately notify the Coordinator if a large volume of records (100+ pages) is anticipated.
5-7 business days from date request received	If a large volume of responsive records is identified, fees are assessed by the Coordinator, the applicant is notified, and the request is placed on hold until a fee deposit is received.
	If it is determined that the responsive records are publicly available, the applicant is notified, and the request is closed.
	If the records retrieval process continues, all responsive records are forwarded to the Coordinator to conduct a scope review.
	The program area subject matter expert(s) is consulted to identify any potentially sensitive or confidential information within the responsive records.
7-10 business days from date request received	Responsive records are assessed for third party or personal information. If consultations are required, notices are sent.
7-25 business days from date request received	Coordinator reviews records and begins preparation of exceptions.
Up to 30 business days from date request received	If third party material requiring a consultation is identified in the responsive records, the Head can approve an extension to the deadline for response to the applicant.
25-28 business days from date request received	If extensions are not applicable, the Coordinator prepares a redline version response package for review and signoff by the Head.
28-30 business days from date request received, unless extended	After signoff process is complete, the Coordinator prepares/sends release package to applicant and closes file.