PENDER ISLAND PUBLIC LIBRARY

Privacy Management Program

Compiled by Carmen Oleskevich, Library Director

Approved June 26, 2024

4407 Bedwell Harbour Road, Box 12, Pender Island BC V0N 2M0
250-629-3722
penderislandlibrary@crd.bc.ca

CONTENTS

1.1 INTRODUCTION

Within BC's Freedom of Information and Protection of Privacy Act (FOIPPA), public libraries fall under the definition of "local government bodies" and therefore are "public bodies" subject to FOIPPA. Each public library is individually responsible for compliance with FOIPPA.

The Pender Island Public Library (PIPL) is responsible for ensuring policies and practices comply with current privacy legislation, including any future amendments made to FOIPPA and its regulations. PIPL must ensure the responsibility for privacy in the Library is understood by all stakeholders, including Trustees, Library Director, staff, volunteers, and service providers.

With the legislative changes to FOIPPA in November 2021, Section 36.2 of FOIPPA requires each public library to develop a "Privacy Management Program" (PMP), in accordance with directions from the BC Minister of Citizens' Services.

PIPL's Privacy Management Program is an evolving set of policies, procedures and tools developed to enable systematic privacy protection throughout the personal information lifecycle. PIPL's PMP is based on the document "Privacy Guidelines for Public libraries", provided by the Public Libraries Branch, BC Ministry of Municipal Affairs, 2023. (Privacy Guidelines for Public libraries).

1.2 HEAD OF PIPL AND PRIVACY OFFICER

The PIPL Board has designated the Library Director as the head of PIPL with delegated authority, under FOIPPA, including the responsibilities and powers related to privacy. The Library Director is the Privacy Officer, responsible for being a point of contact for privacy-related matters, support compliance with FOIPPA, and support development/maintenance for privacy policies and procedures.

Approved: Apr. 26, 2023.

1.3 PIPL PRIVACY POLICY

PIPL has a detailed privacy policy. See Appendix A. PIPL Operational Privacy Policy.

Approved: Oct. 28, 2020

Amended and updated: Feb. 28, 2024

1.4 COLLECTION AND USE OF PERSONAL INFORMATION

PIPL will collect personal information from individuals in a variety of ways and for several purposes. Identifying the purpose for collection is an important aspect of assessing whether the collection is authorized by FOIPPA. The purpose must be stated in a Collection Notice (see Collection Notices section below). PIPL may only collect personal information as allowed by s. 26 of FOIPPA. PIPL must, with limited exceptions, collect personal information directly from the person to whom it pertains.

Examples of types of personal information collected by PIPL:

- contact information to register an individual for a Library card
- the materials borrowed, returned, and overdue by an individual
- limits, holds, and charges attributed to an individual
- security camera recordings of individuals using or near Library facilities
- event registration and attendance
- internal emails, notes, memos, and messages created by Library employees
- Library employee and human resources files
- incident and security reports

Examples of purposes for which personal information is collected:

- to track borrowed materials and administer the catalogue
- to communicate programs, contests, or events to the public
- to process payments, such as unpaid fees, fines, or other charges
- to investigate incidents
- to evaluate and improve programs and services
- to ensure the safety and security of employees, volunteers, patrons, and PIPL property

1.4.1 COLLECTING PERSONAL INFORMATION OF CHILDREN / MINORS

PIPL allows minors under 15 years of age to hold PIPL accounts if an adult co-signs to accept responsibility for the activities on that account, such as incurred fees and fines. Capable minors should be informed at the time of account creation, and ideally through information posed at PIPL or online, that their account personal information will be disclosable to their guardian until they reach the age of 19.

1.4.2 USE OF PERSONAL INFORMATION

Personal information in the custody or control of PIPL must not be "used" by PIPL (or its contracted service providers) for purposes other than those purposes for which the information was collected, except with the consent of the individual or as otherwise authorized by FOIPPA.

1.4.3 CONSENT FOR OTHER USE

Consent for the use of personal information must be obtained when PIPL has personal information in its custody or control, and it wishes to use that information for a new purpose other than the purpose for which that information was collected.

PIPL must consider whether the proposed new use meets one of the three criteria established below. Under s. 32 of FOIPPA, personal information can only be used:

- for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose
- if the individual has identified the information and has consented, in the prescribed manner, to the use of the information
- for a purpose for which that information may be disclosed to PIPL under s. 33.

As set out in FOIPPA Regulation, s. 11, consent for other use must be in writing and be done in a manner that specifies:

- the personal information for which the individual is providing consent
- the date on which the consent is effective and, if applicable, the date on which the consent expires
- the new use of the personal information

Consent by an individual must be freely given and optional and individuals must understand their right to refuse to provide consent.

1.4.4 COLLECTION NOTICES

When collecting personal information, PIPL must provide the individual with a Collection Notice and ensure that the individual is told:

- the purpose for collecting information
- the legal authority for collecting information
- the contact information of an officer or employee of PIPL who can answer questions about the collection

Collection notices should be presented before or at the time of collection.

See Appendix B. Examples of Collection Notices and Forms.

1.4.5 ACCURACY OF PERSONAL INFORMATION

PIPL has a duty to make every reasonable effort to ensure that the personal information is accurate and complete with respect to personal information within the Library's custody or control, that is used by the Library to make a decision that directly affects the individual.

PIPL will ensure accuracy:

For patron information:

- having Library cards expire every 3 years, with staff verifying personal information when

Library cards are renewed.

- staff may perform periodic checks, directly with the individual the information is about or using other authorized avenues, to ensure their library card information is still current and valid.
- staff will complete a thorough review of library card applications to ensure all questions are answered completely.

For staffing purposes:

- Library Director will review applications for employment to ensure all questions are answered completely, document when staff information is collected/received, and document how staff information has been verified.

1.4.6 CORRECTION OF PERSONAL INFORMATION

Upon request by an individual, the Library Director is required to correct (or note requested corrections to) inaccurate or incomplete personal information in its custody or control. Individuals should be able to provide proof that information is wrong or incomplete for a correction to be made.

If no correction is made in response to a request, the Library Director must annotate the information with the correction that was requested but not made. On correcting or annotating personal information, PIPL must notify any other third party to whom that information has been disclosed during the one-year period before the correction was requested.

When correcting or updating personal information, consider all other locations where the same information may reside.

1.5 RELEASE OF PERSONAL INFORMATION

PIPL will only disclose personal information for the purposes set out in FOIPPA s. 33. Examples of common disclosure provisions include:

- with an individual's consent
- for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose (e.g., the disclosure was noted in the Collection Notice)
- to an officer or employee (including volunteers and services providers) of PIPL if the information is necessary for the performance of the duties of the officer or employee or if the information is necessary for the purposes of planning or evaluating a program or activity of the Public Library
- under FOI access request provisions (Part 2 – 'Freedom of Information' of FOIPPA)
- for the purpose of collecting amounts owing to PIPL or the government, or for the purposes of a payment to be made to or by PIPL or the government (e.g., debt)

- to a public body or law enforcement agency in Canada, to assist in a specific investigation
- the Library Director determines that compelling circumstances that affect anyone's health or safety exist
- for a research purpose under a research agreement
- in accordance with an enactment of BC or of Canada that authorizes or requires the disclosure
- to comply with a subpoena, warrant or order issued or made by a court or person in Canada with jurisdiction to compel the production of information in Canada

While FOIPPA s. 33 permits, not requires, disclosure at the discretion of PIPL, some of the purposes may entail a mandatory disclosure (for example, to comply with a court order).

Many minors will have the capacity, competency, and the right to make decisions for themselves, participate in processes affecting them, and provide their own consent. Capacity is determined on a case-by-case basis, but it will generally be the case that minors aged 12 and over are capable of acting for themselves under FOIPPA. PIPL should keep in mind that even a child *under* 12 who is "capable" of exercising their own information rights has the right to do so. PIPL's policy on children should not be applied so rigidly that such a child is not able to exercise their rights under FOIPPA.

1.5.1 CONSENT FOR DISCLOSURE

The required elements of consent for disclosure are set out in s. 11 of the FOIPPA Regulation 28. Consent must be in writing and be done in a manner that specifies:

- the personal information for which the individual is providing consent
- the date on which the consent is effective and, if applicable, the date on which the consent expires
- to whom the personal information may be disclosed
- if practicable, the jurisdiction to which the personal information may be disclosed
- the purpose of the disclosure of the personal information
- consent by an individual must be freely given and optional. An individual should understand their right to refuse to provide their consent.

1.5.2 DISCLOSURE IN PRACTICE

EXAMPLES WHERE DISCLOSING INFORMATION IS APPROPRIATE:

- PIPL has a good relationship with the local police, who routinely ask for information about individuals: to provide personal information to police, there must be a specific investigation underway. Casual disclosures are not authorized.

- If a patron provides consent for a family member to pick up materials on their behalf, for the purpose of delivering the materials to them: if proper consent in the prescribed form is obtained, PIPL may disclose the materials. For ongoing pick-up of materials, PIPL may wish to make a note on the patron's file.

- If the police or the CRA are requesting information about an individual, related to an active investigation file that has nothing to do with PIPL, OR the police are requesting video footage of an individual relating to an incident occurring in or around PIPL: before providing the disclosure, obtain the request in writing (from an official email address or letterhead), including the investigation file number, a signature block or contact information of the requesting officer, and details on how to provide them a secure file transfer, if available

- If an individual has been disruptive or breached PIPL's Rules: PIPL may disclose personal information to other public bodies, including other Public Libraries, or law enforcement agencies, to assist in investigations and proceedings against that individual, if a penalty may result (e.g. being banned from the premises, being fined).

- If PIPL is trying to collect a debt owed by the individual the personal information is about: the disclosure is discretionary (Under FOIPPA s. 33(3)(d)) unless the requester has produced a court order to obtain the information, FOIPPA s. 33(2)(l). Third party personal information (e.g. footage of bystanders) may discretionarily be withheld or disclosed. PIPL may disclose a patron's personal information to whoever necessary in order to collect a debt, receive or make a payment.

- If PIPL initiated contact with the police about an incident that occurred or is occurring in or around PIPL: FOIPPA defines "law enforcement" beyond just policing. It may include policy or rule breach investigations undertaken by the Public Body, provided the investigation or proceeding could lead to a penalty or sanction being imposed (FOIPPA definition of "law enforcement" - Schedule 1). PIPL may disclose personal information to the police to open an investigation into the incident.

- If the Library Director, or delegate, believes there are compelling circumstances that affect someone's health or safety: PIPL may disclose an individual's personal information in these circumstances to whoever necessary, including the individual's family members, law enforcement, or medical personnel.

EXAMPLES OF DISCLOSING PERSONAL INFORMATION OF MINORS

Common situations:

- If there has been an accident affecting a child at the Public Library, or someone has made threats about the safety of a child in the Public Library: PIPL may disclose personal information if the head of the Public Library determines that compelling circumstances that affect anyone's health or safety exist (FOIPPA s.33(3)(a)). This disclosure could be to anyone

necessary, including law enforcement, medical professionals, or parents/guardians. Note that the Library Director, or their delegate, must make the disclosure determination in these cases.

- If a guardian is phoning to ask if their minor child is at the Library: the guardian may not be asking about recorded personal information that is subject to FOIPPA. You may tell the guardian that they are free to come into the Public Library to look for their child but patron attendance is not information the Public Library collects. The Library may choose to assist by making an announcement to see if the minor would like to approach staff or contact their guardian directly.
- If a guardian is asking for information about their minor child's account, and the guardian is named on the account: staff should verify the guardian's identity. If by phone, with two or three verifying questions using the information recorded on the file and if in person, by checking ID. Once identification is verified, the staff may disclose the information on the minor's account.
- If a guardian who is NOT named on their minor child's account is asking for information about the child: even guardians who are not named on the account will have rights to access their minor child's personal information for 'incapable' minors and for children under the age of 12, as set out above. For capable minors aged 12 and over, the staff should inform the guardian that because they are not named on the account, the Library cannot disclose the personal information. The Library can suggest that the guardian provide the minor's consent for the disclosure or authorization to be added to the account or obtain the information from the named guardian. The Library should seek proof of guardianship and verify identity before disclosing information.

1.5.3 FREEDOM OF INFORMATION (FOI) ACCESS REQUESTS

The public has a right of access to all records in the custody or under the control of PIPL, subject to exceptions. Routine information access or correction, such as access to borrowing history or a change of address, may be facilitated by any employee or volunteer with authority. Non-routine requests for access or correction should go through the Library Director (Privacy Officer).

ACCESS TO ROUTINE INFORMATION (INFORMAL ACCESS REQUEST)

Where possible, individuals should be given routine access to their own personal information, such as their borrowing history (if applicable) and current address on record. Care is needed to ensure that it is the individual the personal information relates to who is gaining access.

Access by employees or volunteers to patron information should be on a need-to-know basis only and based on their job duties. Employees or volunteers who are authorized to help individuals access their own personal information should only do so when individuals are having difficulties accessing the information on their own.

ACCESS TO NON-ROUTINE INFORMATION (FORMAL FOI ACCESS REQUEST)

An individual may submit a formal access request for records under Part 2 – 'Freedom of Information' of FOIPPA. This could include a request for the applicant's own personal information, or for a general record of PIPL such as copies of contracts or internal communications.

Records that are exempt from FOI Access Requests include:

- a record that is available for purchase by the public
- a record that does not relate to the business of PIPL
- a record of metadata

PIPL has a duty to assist applicants (to respond openly, accurately, completely and without delay), conduct an adequate search for records, ensure records are redacted as required by Part 2 – 'Freedom of Information' of FOIPPA, and respond to a request within 30 business days of receiving the request (unless extended under the provisions set out in FOIPPA).

PIPL will confirm an individual's identity before providing records about that individual.

FEES FOR ACCESSING A RECORD

PIPL may charge an applicant a prescribed application fee for FOI Access Requests, unless the request is for an individual's own personal information. Additional processing fees may also be applied, depending on the size and complexity of the request description. The maximum fees for services provided is set out in the FOIPPA Regulation, Schedule 1. Fees may be charged for the following tasks or services:

- locating, retrieving and producing the record
- preparing the record for disclosure
- shipping and handling the record
- providing a copy of the record

There are no processing fees charged for:

- the first three hours spent locating and retrieving a record
- time spent severing (removing) information from a record

PIPL will give an applicant a written estimate of the total fees before providing the services and may require an applicant to pay a deposit in an amount set by the Library Director. Applicants may provide a written request to excuse payment of all or part of the fees. The Library Director may excuse payment, if, in their opinion, the applicant cannot afford the payment or for any other reason it is fair to excuse payment, or the record relates to a matter of public interest, including the environment or public health or safety. A person who has legal care of a minor under 12 years of age may on behalf of the child exercise the child's following rights under *FOIPPA*, if the minor is incapable of acting under that provision:

- making an FOI access request on behalf of the minor
- authorizing the indirect collection of information about the minor
- requesting a correction to personal information about the minor
- consenting to a specific use of the minor's personal information

- consenting to the disclosing of the minor's personal information

1.6 RETENTION AND DISPOSAL OF PERSONAL INFORMATION

1.6.1 RETENTION OF PERSONAL INFORMATION

PIPL will retain an individual's personal information for at least one year after the information is used to make a decision that may directly affect the individual. To minimize the risks of unauthorized use and disclosure of personal information in PIPL's custody or control, PIPL will not retain personal information that is no longer required for operational, legal, or archival reasons.

1.6.2 DISPOSAL OF PERSONAL INFORMATION

The following procedures will be used to securely dispose of personal information, both in hardcopy and electronic form.

- Paper: will be shredded (ideally using a cross-shredder). Paper with personal information will not be disposed into a recycle bin.
- Electronic data: Obsolete computer files and emails will be deleted, and computer trash bins emptied regularly. Computer files will then be purposefully overwritten, wiped, or sanitized. PIPL will seek assistance from IT professionals to develop procedures for data erasure to ensure materials are removed from server backups.
- Public Computer Workstations: For INTERNET SEARCH HISTORY LOGS, PIPL has installed security software that automatically purges the cache and history folders on public computers after each user session. For lendable tech, information saved on lendable laptops is cleared before circulating to the next patron.

See Appendix D. PIPL Procedures for Disposal of Personal Information.

1.7 SECURITY MEASURES

PIPL protects the personal information it holds by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. PIPL employs administrative, physical, and technical security measures.

1.7.1 ADMINISTRATIVE SECURITY MEASURES

PIPL protects the personal information it holds by making "reasonable security arrangements" against such risks as unauthorized access, collection, use, disclosure or disposal. Security arrangements can be administrative / procedural, physical, or technical, and apply to prevent breaches both from within and from outside of PIPL.

LIBRARY CARDHOLDER RECORDS

PIPL is a member of the BC Library Cooperative (BCLC) which provides the Sitka Evergreen integrated library computer system. The Sitka Evergreen database contains personal information

on all library card holders. All library users have a right to privacy and confidentiality when using Sitka Evergreen public access catalogues or when interacting with library staff in their operation of Sitka Evergreen. Complete details are available in the BCLC Sitka Policy Manual (Sitka (shared library database) Detailed Privacy Policy).

PIPL has implemented role-based access to Sitka Evergreen and other technology resources as a security control to limit who has access to what information, in accordance with need-to-know and least privilege principles, ensuring that (wherever practicable) employees and volunteers have access only to the minimum amount of personal information they require to perform their employment duties. Access permissions to Sitka Evergreen are documented, remain up-to-date, and assigned on a consistent basis.

Need-to-know access is restricted to only those employees and volunteers who require access to carry out their work. The need-to-know principle will be implemented in various ways, such as:

PIPL has installed technical access controls for:

- Sitka Evergreen, including patron accounts, circulation history, and Holds
- Interlibrary loan (ILLUME) requests and website administration
- computer admin access for maintenance tasks
- other

PIPL will restrict access for casual staff, students, and volunteers to only that information which they need to carry out their work. The intention of the least privilege principle is to limit the damage that can result from accidental or unauthorized use. Employees and volunteers are not entitled to access information merely because of status, length of service, rank, or office.

Examples of restricting access

- Patron name, barcode, contact information - only accessible to employees or volunteers who check out materials, update personal information, or place holds for patrons
- Patron borrowing history – only accessed when assisting patrons to look up their own information. Employees and volunteers should be discreet and avoid looking at the information themselves where possible.
- Home Service patron's disability information, reading preferences, and borrowing history - only employees and volunteers who make selections for Home Service patrons and update their personal information

PIPL will annually review employee and volunteer access levels to Sitka Evergreen and employee records to track who has access to files containing sensitive information.

EMPLOYEE RECORDS

PIPL has restricted access to employee records to only those employees who require access to carry out their work. Examples of restricted access:

- physically segregated, and controlled access to, employee records
- established which individuals may access certain employee and patron records
- installed technical controls for access to online HR and payroll software programs

- Employee timesheets - only Library Director or designate responsible for supervising employees and/or payroll.
- Employee criminal record check reports - only Library Director or designate responsible for screening employees in this regard
- other

Employees are not entitled to access information merely because of status, length of service, rank, or office.

PIPL will annually review employee access levels to employee records to track who has access to files containing sensitive information.

TRAINING AND AWARENESS

The Library Director will ensure each new employee and volunteer receives training on privacy policies and procedures, including how and when to report a privacy breach to the Library Director. Existing employees and volunteers will receive regular updates on privacy training.

CONFIDENTIALITY AGREEMENTS

PIPL implements confidentiality agreements with employees and volunteers who are authorized to access personal information. The confidentiality agreements stipulate that the employee or volunteer will comply with the requirements of FOIPPA and PIPL's privacy policies when dealing with personal information and stipulate what steps may be taken to enforce the policies.

All PIPL Employee Agreements include a clause on privacy declarations and require the employee's acknowledgement of privacy responsibilities upon acceptance of employment. Further details on privacy responsibilities are outlined in the PIPL Human Resource Policy for Employees, Section 1. Terms of Agreement: Confidentiality.

All PIPL volunteers are required to acknowledge and sign a "Declaration of Volunteer Commitment to PIPL Policies", including a clause committing to protecting confidential information. Further details of volunteer privacy commitments are outlined in the PIPL Volunteers Management Manual.

SERVICE PROVIDERS

Contracts with service providers may include the details of security measures, as well as an acknowledgement that the service provider understands their requirements under FOIPPA. Where contracted services are used for storage, transportation or destruction of records, PIPL will require the contractors to provide a certificate of destruction.

1.7.2 PHYSICAL SECURITY MEASURES

PIPL physical security measures include:

- storing records containing sensitive information in locked filing cabinets, with controls over distribution of keys.
- providing a locked cabinet for library users records, with keys distributed to designated staff
- providing a locked cabinet for workers' records (employee, Trustees, volunteers) and financial records (CRA, SOFI, WCB, donations, etc.) with keys distributed to Library Director and Bookkeeper
- positioning of computer screens with financial and employee record so they are not visible to others.

1.7.3 TECHNICAL SECURITY MEASURES

PIPL ensures that internal or contracted IT personnel are aware of PIPL's legal duty to protect and secure records containing personal information. The following personnel are responsible for technical measures:

- BC Libraries Cooperative staff for the Sitka Evergreen computer system
- Capital Regional District (CRD) IT Support staff for PIPL staff computer workstations
- IT Support contractors for PIPL public computer workstations

1.8 PRIVACY IMPACT ASSESSMENTS (PIA)

A Privacy Impact Assessment (PIA) is a step-by-step review process to make sure that a public body is meeting its privacy requirements under FOIPPA and helps a public body identify and mitigate any privacy risks involved in a particular initiative.

See the Privacy Impact Assessment Template for "non-ministry public bodies" available through the BC Government website: Guidance for Privacy Impact Assessments

1.9 PRIVACY COMPLAINTS

1.9.1 TYPES OF COMPLAINTS

PRIVACY COMPLAINTS

- unauthorized collection of personal information;
- unauthorized use of personal information;
- unauthorized disclosure of personal information;
- inadequate security of personal information; or
- refusal to correct or annotate records containing personal information.
- PIPL may be asked to explain their legal authority to do what they did.

FOI ACCESS COMPLAINTS

- a failure to make a reasonable effort to assist an applicant;
- an inadequate search for records in response to a request for records;
- an inappropriate fee assessment;
- a refusal to waive an assessed fee; or

- an unauthorized extension of time taken by the Public Library to respond to an access request.

PIPL will make relevant policies and procedures on collection of personal information available to the public.

1.9.2 PIPL'S RESPONSE TO PRIVACY COMPLAINTS

PIPL may confer with the Office of the Information and Privacy Commissioner to provide guidance in response to a complaint.

PRIVACY COMPLAINT PROCEDURES

- Front line staff are normally the first point of contact for public complaints
- Staff will recognize when the issue is a privacy complaint about how an individual's personal information has been handled by the Library
- Staff will instruct the complainant to the following steps:
- The first step is for individuals to attempt to resolve the complaint directly with PIPL.
- Complaints must be submitted in writing and addressed to the PIPL Privacy Officer (Library Director).
- Complaints should provide as much detail as possible to assist the Privacy Officer to understand the nature of the complaint.
- The Privacy Officer has at least 30 business days to respond to a privacy complaint. (*The Office of Information and Privacy Commissioner (OPIC) will generally not accept complaints until at least 30 business days have passed for a response between complainant and an organization*.)
- The Privacy Officer will:
  - determine the type of privacy complaint (Privacy vs. FOI Access)
  - will research the issue and gather additional information as needed from staff and the complainant
  - will attempt to demonstrate to the complainant that policies, procedures, or guidelines were followed, and show that collection, use, or disclosure was authorized
  - will keep copies of correspondence with complainant for internal use, and to work with OPIC if needed.
- If PIPL is unable to resolve the complaint with the individual directly, we will inform the individual of their right to escalate their complaint to the OIPC Commissioner. The OIPC may investigate the complaint and make findings, including whether PIPL complied with FOIPPA.

PIPL can provide the following link for more info: *How do I make a complaint? - Office of the Information and Privacy Commissioner for BC (oipc.bc.ca)*

1.10 PRIVACY BREACHES

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure, or disposal of personal information in contravention of FOIPPA. The most common privacy breaches happen when personal information of patrons or employees is stolen, lost, or mistakenly disclosed.

The Library Director will notify an affected individual if a privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or other significant harms as described in FOIPPA, section 36.3. The Library Director is also required to notify the Office of Information and Privacy Commissioner when the significant harm threshold is met.

1.10.1 REPORTING PRIVACY BREACHES TO PIPL

PIPL has implemented the following procedures for employees and the public to report privacy breaches to PIPL:

1. Identify and contain the breach
2. Report the breach to the appropriate people at PIPL
3. Consider notification to affected individuals
4. Investigate the circumstances around the breach
5. Develop mitigation strategies to avoid the breach in the future
6. Document the steps taken throughout the process

In developing response procedures, PIPL will consult the OIPC (BC) Guide Document: Privacy Breaches: Tools and Resources.

1.10.2 REPORTING A PRIVACY BREACH TO OIPC

PIPL will notify the commissioner of the OIPC if a privacy breach could reasonably be expected to result in significant harm to an individual.

For more information, consult: OIPC (BC) Guide Document: Privacy Breaches: Tools and Resources

See Appendix C. Examples of Privacy Breach Notifications.

APPENDIX A. PIPL OPERATIONAL PRIVACY POLICY.

PIPL Operational Policy Manual

Section 3. Membership

Section 3.2 Privacy

Personal information is collected by the Pender Island Public Library (PIPL) under the authority of the BC Library Act and section 26 of the Freedom of Information and Protection of Privacy Act (FOIPPA). Any personal information collected, used, or disclosed by the PIPL is in accordance with FOIPPA, and PIPL is committed to protecting members' confidentiality and personal privacy. All staff, volunteers and students sign a declaration of commitment to confidentiality before beginning work at PIPL.

3.2.1 Purposes for Which Personal Information may be collected

The primary purposes for which the PIPL collects personal information are:

- the proper administration of Library services and programs
- the planning and evaluating of services and programs
- other purposes consistent with and pertaining to library services and programs

Other purposes include, but are not limited to:

- providing access to library materials, services, and programs
- communications
- collection of fines and fees
- evaluating and improving services
- protection of Library property
- security of users and staff

Except in the limited circumstances provided for in FOIPPA, personal information about an individual will be collected directly from that individual. Individuals are informed of the reasons for collecting personal information at the time (or before) it is collected. At the time of collection (or before), individuals are informed of the PIPL's legal authority for collecting the information, and the name, title, and contact information for the Library's Privacy Officer, who is responsible for ensuring compliance with FOIPPA. Questions about the library collection can be directed to the Privacy Officer.

3.2.2 Integrated Library System

PIPL is a Member of the BC Library Cooperative (BCLC) which provides the Sitka Evergreen integrated library computer system (ILS). All library users have a right to privacy and confidentiality when using Member library public access catalogues or when interacting with Member library staff in their operation of Sitka's ILS. Complete details are available in the BCLC Sitka Policy Manual, and the following is adapted from that manual.

Personal information collected includes information related to registration, such as name, address, phone number, and circulation records, including information that identifies materials

checked out by a patron. It includes any library record about an identifiable patron or individual. By providing an email address at the point of registration in the ILS, patrons consent to receive notices (Courtesy (Pre-due) and Overdue notices) via electronic mail.

When a library user visits the library's public access catalogue, the IP address of the computer or internet provider and related site visit information may be collected. This information is only used in statistical (non-personal) form to help make improvements to the website.

Member libraries do not sell or rent personal information collected in the ILS. Personal information is disclosed only in accordance with FOIPPA. The Member library will retain a link between the patron record in the ILS and items returned for a reasonable period to ensure returned items are complete and in good condition. The library may store other personal information in the patron database but only where required. This may include answers to patron questions and logs that monitor use and possible abuse of the library borrowing policy or for related operational and statistical needs.

Member libraries will make all reasonable efforts regarding personal information collected and stored in the ILS in order to:

• minimize the amount of personal information collected and stored

• render it anonymous where feasible

• retain it for the minimum time necessary

• protect it from unauthorized access, use or disclosure

• destroy it securely when no longer needed

Personal information relating to a library user may only be used by library employees working within the scope of their duties on a need-to-know basis. A more detailed version of BCLC's Privacy Policy concerning Members and information collected may be obtained upon request.

3.2.3 Protection of Personal Information

The PIPL uses reasonable security measures to mitigate and protect against risks such as unauthorized access, collection, use, disclosure, or disposal of personal information. Measures include administrative, physical, technological, and operational safeguards that are appropriate to the nature and format of personal information. PIPL will not retain any personal information longer than necessary for the provision, evaluation, and planning of library services and programs. Employee and business records will be retained in accordance with federal and provincial rules.

3.2.4 Access, Accuracy and Correction

Members of the public have access to their own personal information. Upon request, access to recorded personal information about a member of the public is provided to that individual upon verification of identity. To request access to personal information, the member must submit a written request to PIPL's Privacy Officer. The request should provide enough detail to enable a Library employee to find the personal information. PIPL will endeavour to ensure the personal information is accurate, complete, and up to date. Members have the right to request that their

personal information held by the PIPL be corrected if the member believes it is inaccurate. The member may do so by submitting a request in writing to the Privacy Officer.

3.2.5 Minors

Children have the same rights as adults with respect to their personal information under FOIPPA. Where a child is "incapable" of exercising their right to access, correct or consent to the disclosure of their personal information, the child's parent or guardian may do so on their behalf. PIPL assumes that children 12 years and older are generally capable of exercising their own rights for policy purposes. However, PIPL may treat a request on an individual basis where a child or parent/guardian does not believe the guideline age is appropriate in their circumstances.

3.2.6 Disclosure

The PIPL will not rent or sell personal information. PIPL will not disclose personal information to third parties except in accordance with the exceptions permitted under FOIPPA, including the options below or with an individual's consent.

i. Collecting a Debt

The PIPL may disclose personal information to a collection agency or credit bureau for the purpose of collecting debt.

ii. Emergency Situations

PIPL may disclose personal information under emergency or compassionate circumstances; for example, so that next of kin or a friend of an individual who is injured, ill, or deceased can be contacted.

iii. Service Providers to the Library

PIPL ensures that any service providers requiring access to personal information to deliver services on behalf of PIPL treat personal information in compliance with FOIPPA. Providing some library products and services may require that PIPL share personal information with a service provider, and/or that an individual shares personal information when creating a separate account with the service provider.

iv. Police/Law Enforcement

Personal information may be disclosed to comply with a subpoena, a warrant, or an order by a court, person, or body in Canada with the jurisdiction to compel the production of information, or to respond to a specific written request from a law enforcement agency to assist in a specific investigation, or as required by law.

3.2.7 Retention

Personal information is kept for varying periods of time depending on the purpose for which the information was collected. If PIPL uses personal information to make a decision that affects library users, PIPL must keep that information for at least one year so that users have an opportunity to access it. Otherwise, PIPL will keep personal information only for the length of time necessary to

fulfill the purposes for which it was collected. Personal information is securely destroyed when it is no longer needed.

3.2.8 Changes to this Privacy Policy

PIPL's practices and policies are reviewed from time to time. This policy will be updated to reflect the changes.

3.2.9 Privacy Officer Contact

For questions or concerns about this policy or how the PIPL handles the personal information collected, please contact:

Library Director

Box 12, 4407 Bedwell Harbour Rd.

Pender Island BC V0N 2M0

Phone: 250-629-3722

Email: penderislandlibrary@crd.bc.ca

PIPL motion approved: Feb. 28, 2024

APPENDIX B. PIPL INFORMATION COLLECTION NOTICE AND FORMS.

POSTED COLLECTION NOTICES

A PIPL Collection Notice is posted at key service areas in the library:

INFORMATION COLLECTION NOTICE

Your personal information is collected by the Pender Island Public Library under the authority of BC's Freedom of Information and Privacy Act Section 26, and the BC library act, for the purpose of administering your library registration and providing you library services. The personal information collected includes full name, phone number, email address and physical address.

Should you have any questions about the collection of this personal information please contact Carmen Oleskevich, Privacy Officer, coleskevich@crd.bc.ca, 250-629-3722.

Pender Island Public Library

I ♥ My Library

PENDER ISLAND · BC

INFORMATION COLLECTION FORMS

PIPL Information Collection forms include those for new library cards, program registration, and newsletter recipients.

PIPL membership/ library card forms will contain the following notice:

***NOTE**: The information on this form is collected by Pender Island Public Library under the authority of BC Library Act and BC Freedom of Information and Protection of Privacy Act, s.26. The information will be used to administer your Library account including assessing your eligibility for borrowing privileges, which may involve enquiring into your debt status with other public libraries, to contact you about reserve materials, or to collect overdue materials. For questions about the collection or use of this information, please contact the Library's Privacy Officer at penderislandlibrary@crd.bc.ca, 250-629-3722.*

APPENDIX C. PROCEDURES FOR DISPOSAL OF PERSONAL INFORMATION

The following schedule guides PIPL staff regarding the disposal of personal information.

The following procedures will be used to securely dispose of personal information, both in hardcopy and electronic form.

Paper Documents

Every 6 Months:

- Paper documents, including Interlibrary Loan Requests, Hold Notifications, Membership Applications, Overdue Reports, and others will stored in a locked file cabinet or in the collection bin designated for shredding in the main office area, and shredded after 6 months.
- Paper documents containing personal information will not be disposed of in a recycle bin.

Electronic Data

Every Month

- Electronic data held in Sitka Evergreen database, including expired Patron Accounts, Overdue reports, and statistical reports will be deleted and computer trash bins emptied regularily.
- Electronic data stored on staff computers, including obsolete computer files and emails will be deleted and computer trash bins emptied regularily. PIPL will seek assistance from IT professionals to develop procedures for data erasure to ensure materials are removed from server backups.

After Every User

- Public Computer Workstations: For INTERNET SEARCH HISTORY LOGS, PIPL has installed security software that automatically purges the cache and history folders on public computers after each user session.
- For lendable equipment, information saved on lendable laptops is cleared before circulating to the next patron.

APPENDIX D. EXAMPLES OF PRIVACY BREACH NOTIFICATIONS.

1. Minor security breach at BC Libraries Cooperative

As we take our patrons' privacy very seriously, we want to inform you of a brief minor security breach incident that occurred on April 19th to our library operating system, SITKA. The leaked data was limited to email addresses or phone numbers of people who received automated messages such as such as holds notifications from SITKA from March 27th to April 19th. No individual library information, other identifying information, contents or subject lines of emails, or any information about people's checkouts, holds or fines were leaked. The BC Libraries Co-op that operates SITKA believes the main harm that can come from the leaking of this information is a potential increase in spam, phishing or spear phishing attacks. We have not had any reports of any issues yet. Please contact our Library Director (name) if you have any concerns or if you have experienced any problematic communication.

2. (Date) Breach Incident

Suggested Public Catalogue Banner Text:

If you received an email or SMS notification from us between March 27 and April 19, 2024, your email address or phone number may have been leaked. Click here for more information.

Suggested Website Post Text:

Notification of Privacy Breach

On April 25, 2024, our ILS (integrated library system) provider notified us that they had experienced a privacy breach. Log files on their servers were obtained that contained the email addresses and phone numbers of patrons who had received automated notifications from the library system (i.e., checkout notices, overdue notices, hold notifications) between March 27 and April 19.

Only the email addresses of people who received notifications (or the phone number of people who received SMS notifications) were leaked. The content of the notifications was NOT leaked. The leaked data does not say what the notifications were about, and it does NOT reveal any other information about patrons or their library use, such as checkouts and holds. We regret this happened and are working with the software provider to ensure this issue is resolved and does not occur again.

It is our understanding that the most likely risk from this information leaking is it being used to generate spam or phishing messages. We highly recommend you refer to https://antifraudcentre-centreantifraude.ca/scams-fraudes/phishing-hameconnage-eng.htm for more information.

In addition, it may increase the likelihood of spear phishing messages – messages pretending to be from a person or system you are known to communicate with. Please know that the library will NEVER ask you for your password nor any other sensitive email like social insurance or banking information, nor ask for funds from you.

If you receive any message that appears to be from the library but is asking for any of these things, do not hesitate to follow up by calling us directly at (xxx)xxx-xxxx if you are at all unsure of its truthfulness.