2023

Privacy Guidelines for **BC Public Libraries**

bit.ly/45E3fCk

Legal Notice

These guidelines are a collaboration between the Public Libraries Branch and Ministry of Education and Child Care/Municipal Affairs Privacy Officers and were reviewed by the Privacy, Compliance and Training Branch at BC's Ministry of Citizens' Services.

This document is does not constitute legal advice on privacy matters.

Questions not addressed in this document can be directed to the BC Government's Privacy Helpline: 250-356-1851, Privacy.Helpline@gov.bc.ca or Office of the Information Privacy Commissioner for British Columbia.

Legal Review and editing provided by Erika Decker Brimacombe, J.D.

ROLE OF THE PUBLIC LIBRARIES BRANCH AT THE MINISTRY OF MUNICIPAL AFFAIRS

Through the administration of the *Library Act* [RSBC 1996] c. 264, the Public Libraries Branch strengthens the Public Library system by providing strategic leadership, professional advice, funding, and coordinating province-wide programs and shared services.

These guidelines promote effective governance by supporting BC Public Libraries' compliance with *FOIPPA*.

Table of Contents

INTRODUCTION

Purpose

These guidelines are intended to:

- Provide an overview of public libraries' privacy obligations
- Assist with the development of a public library's privacy policy

These guidelines will introduce a wide range of privacy-related information to British Columbia's Public Libraries. They are based on the globally recognized privacy principles that underpin B.C.'s privacy legislation, including the ***Freedom of Information and Protection of Privacy Act*** (RSBC 1996, c. 165) (FOIPPA) and privacy best practices for demonstrating compliance[1] . These guidelines will give you an overview of the FOIPPA requirements and how Public Library operations may comply with them. They are intended to help the reader be aware of the privacy implications that may arise in day-to-day functions, to practice due diligence and to be proactive by clearly communicating expectations to staff and patrons. They can help Public Libraries create or update their privacy policies and procedures.

Each Public Library must:

- be responsible for ensuring their policies and practices comply with current legislation, including any future amendments made to *FOIPPA* and its regulations that may not be reflected in these guidelines.
- ensure the responsibility for privacy in Public Libraries is understood by trustees, directors, service providers, staff, and volunteers.
- use its own judgment in making decisions based on privacy legislation, principles, and best practices.

1 For more information about privacy principals and best practices from the BC Government:
• Ten Principals of Privacy Protection
• Privacy & Personal Information in the Public Sector

Privacy Legislation in B.C.

In B.C., different privacy legislation applies to **public** sector organizations (including Public Libraries) and **private** organizations.

- Public Libraries fall under the definition of "local government bodies" in *FOIPPA*, and therefore they are "public bodies" subject to *FOIPPA*. Each Public Library is individually responsible for compliance with *FOIPPA*.
- B.C.'s ***Personal Information Protection Act*** [SBC 2003] c. 63 (PIPA) applies to private sector organizations[2] (such as a businesses or corporations, unions, political parties, and not-for-profits[3]) and is out of scope of this document.
- B.C.'s ***Privacy Act*** [RSBC 1996] c. 373 covers civil disputes between private citizens and is outside of the jurisdiction of the Office of the Information and Privacy Commissioner (OIPC) and is outside the scope of this document.

Application of *FOIPPA*

As the name suggests, the *Freedom of Information* and *Protection of Privacy* ***Act***:

1. establishes an individual's **right to access** records in the custody or control of a Public Library, including access to a person's own personal information; and
2. **protects personal privacy** by setting out the terms under which a Public Library collects, uses, retains, protects and discloses the personal information of individuals.

FOIPPA applies to all records held in the "custody or under the control[4] " of the Public Library.

CUSTODY

The record is physically in the Public Library's possession.

CONTROL

The Public Library has the power or authority to manage the record, even if it is in the custody of another organization (for example, the records retained by a Public Library's service provider)

Some specific types of records are exempt from *FOIPPA*, including research material and court records[5]. *FOIPPA* applies to all employees, officers, directors, volunteers, and service providers of the Public Library.

2 Most of a Public Library's contracted service providers would fall under *PIPA* independently, except for the services provided to a public body under contract. The service provider is subject to and must comply with *FOIPPA* with respect to personal information collected, used, retained, stored, and disclosed on behalf of the Public Library.

3 "Friends of the Library", "BC Library Trustees Association" and "BC Library Association" are examples of an organizations that are covered under *PIPA*. These types of organizations are outside the scope of this document.

4 For detailed definitions for "custody" and "control", see the BC Government's *FOIPPA* Policy Definitions

5 See *FOIPPA* s. 3(3) - 3(6) for complete list of out-of-scope records.

DEFINITIONS

See also the *FOIPPA* definitions in Schedule 1 of the *Act*.

contact information – 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. This type of business contact information is excluded from the definition of "personal information" under *FOIPPA*.

employee – Under *FOIPPA*, the definition of "employee" (in relation to a Public Library) includes volunteers and a service providers.

FOI Access Request – A request made by an individual for access to information under Part 2 – 'Freedom of Information' of *FOIPPA*.

personal information – Recorded information about an identifiable individual other than business contact information, such as: name, image, personal telephone number, home address, identification numbers, date of birth, amounts owing, opinions, materials borrowed, etc.

personal information bank –An aggregation of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Privacy Impact Assessment ("PIA") – An assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 – 'Protection of Privacy' of *FOIPPA*. Public Libraries must conduct PIAs in accordance with the directions of the Minister of Citizens' Services[6].

Privacy Officer – The individual who is designated to manage the Public Library's compliance with *FOIPPA*.

Public Library – Public Libraries are defined as "local government bodies" under *FOIPPA*, specifically a "library board as defined in the *Library Act*". Local government bodies are public bodies under *FOIPPA*.

record – Includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other item on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

service provider – A person or business retained under a contract to perform services for a Public Library. It includes employees, subcontractors of service providers and their associates[7] who have access to personal information and who may use and disclose this information on behalf of a Public Library.

6 Minister of Citizens' Services Direction 2-21,"Privacy Impact Assessment Directions"

7 Under s. 3(2)(b), *FOIPPA* also applies to "associates" of service providers. See the full definition of "associate" in relation to a service provider in *FOIPPA* – Schedule 1

SUMMARY OF KEY *FOIPPA* REQUIREMENTS

Each Public Library must:

- officially designate a 'head' of the Public Library, and set out in writing any delegation of the head's authority under FOIPPA (page 9)
- develop a "**Privacy Management Program**", in accordance with the directions from the Minister of Citizens' Services (page 10)
- implement **mandatory privacy breach notifications** (page 27)
- make available to the public the Public Library's privacy policy and any Public Library rules, policies, manuals, instructions, or guidelines if the record is for the purpose of administering a program or activity that affects the public (page 10)
- make publicly available a directory that lists the Public Library's personal information banks, also known as a "Personal Information Directory" (page 11)
- only collect, use, or disclose personal information as authorized by *FOIPPA* (page 12)
- provide individuals with Collection Notices when collecting personal information from them (page 13)
- ensure the accuracy of personal information and respond to requests to correct personal information (page 18)
- make reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or disposal (page 20)
- retain personal information for at least one year after it is used to make a decision that directly affects the individual that the information is about (page 22)
- respond to Freedom of Information (FOI) Access Requests (page 26)
- conduct Privacy Impact Assessments ("PIAs") in accordance with the Minister of Citizen's Services Directions for all new initiatives or before any significant change to an initiative of the Public Library (page 29)
- if relying on consent, obtain that consent in writing in the prescribed form (template available on page 39

ACCOUNTABILITY AND TRANSPARENCY

Delegated Authority

Under *FOIPPA*, the "head of the public body" (i.e., the head of each Public Library) holds specific responsibilities and powers related to privacy for the Public Library. For example, the head of the public body responds to FOI requests, makes disclosure decisions, and must correct or annotate inaccurate information in a record.

Any duty, power, or function the head of a public body has under *FOIPPA* (except the power to delegate), may be delegated by the head to any person.[8] The delegation **must be in writing** and may contain any appropriate conditions or restrictions. A Privacy Officer does not have the power to act on behalf of the head of the Public Library under *FOIPPA* unless they have been delegated that power in writing.

Who acts as the head of the Public Library with respect to *FOIPPA* must be determined by each Public Library, and set out in a bylaw, policy, or other legal instrument by which the Public Library acts. [9]Typically, this is the Director or Chief Librarian.

Role of a Privacy Officer

Each Public Library is responsible for personal information in its custody or control and should designate an individual or individuals who are responsible for ensuring the Public Library's compliance with *FOIPPA*.

Public Libraries will need to appoint an individual to be the Public Library's Privacy Contact, who can:

- ensure that privacy principles and requirements are clearly identified and communicated to staff and to the public
- provide training and awareness activities that support the ability of staff to monitor their own compliance, to foster a culture of privacy best practices within the Public Library
- ensure Public Library privacy policies and procedures are implemented and kept current
- ensure adequate resources are identified to support privacy policies
- ensure privacy protection is "built in" to all processes that involve personal information
- assist in conducting privacy impact assessments
- maintain the Public Library's personal information directory
- guide the development and implementation of reasonable security arrangements and ensure they are kept current
- respond to privacy complaints, breaches, and requests to access or correct information

If there is no designated Privacy Officer in the Public Library, these responsibilities should be assumed by the head of the Public Library. Using these guidelines will help prepare for *FOIPPA* compliance and help address privacy issues and questions that may arise.

8 *FOIPPA* s. 66. A template is available at Province of British Columbia (gov.bc.ca) to assist public bodies in the broader public sector in delegating duties, powers, or functions of the head of the public body under section 66.
9 *FOIPPA* s. 77.

Privacy Management Program

With the legislative changes to *FOIPPA* in November 2021, a new provision was added. Section 36.2 of *FOIPPA* will require each public body to develop a "Privacy Management Program" (PMP), in accordance with directions from the Minister of Citizens' Services.

A PMP is an evolving set of policies, procedures and tools developed by a public body to enable systematic privacy protection throughout the personal information lifecycle.

PMP directions and guidance are available at Privacy & Personal Information Resources - Province of British Columbia (gov.bc.ca)

Transparency — Communicating Policies and Practices to Patrons

Demonstrating a Commitment to Privacy

How to inform patrons about privacy policies and procedures:

- Include brief privacy statements on Public Library cards and refer patrons to the Public Library's online privacy policies and procedures for more information.
- Post privacy notices at service desks and information boards.
- Provide a link on the Public Library's homepage to the privacy policy and related information.

Public Libraries must let individuals know how they can access information about the Public Library's privacy policies and procedures when requested. While the privacy policies are not *required* to be posted online, it is common and efficient to do so. A Public Library should make readily available to the public the information about its policies and practices relating to the management of personal information.

Moreover, any Public Library rules, policies, manuals, instructions or guidelines must be made available to the public if the record is "for the purpose of administering a program or activity that affects the public". [10] Individuals requesting to see these records do not need to make a formal FOI Access Request to see them, and the records should be producible in a much shorter time-frame than formal FOI Access Requests. Ideally, most records established as routinely releasable to the public should be available on demand.

Examples of privacy policies, procedures, and other guiding documents that Public Libraries should consider developing and publishing include:

- Privacy Policy
- Records Management Policy (how information is organized, retained, and disposed), and Records Retention Schedules
- FOI Access Request Procedures
- Directory of Personal Information Banks (required – see below)
- *FOIPPA* Delegation of Authority
- Privacy Complaints and Breaches Procedures

10 *FOIPPA* s. 70.

Directory of Personal Information Banks

Public Libraries are required to provide the public with information about what kind of personal information the Public Library has and for what purpose it has that information.[11] Public Libraries must make publicly available a directory that lists the Public Library's personal information banks, also known as a "Personal Information Directory" (PID).

Personal information bank

an aggregation of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

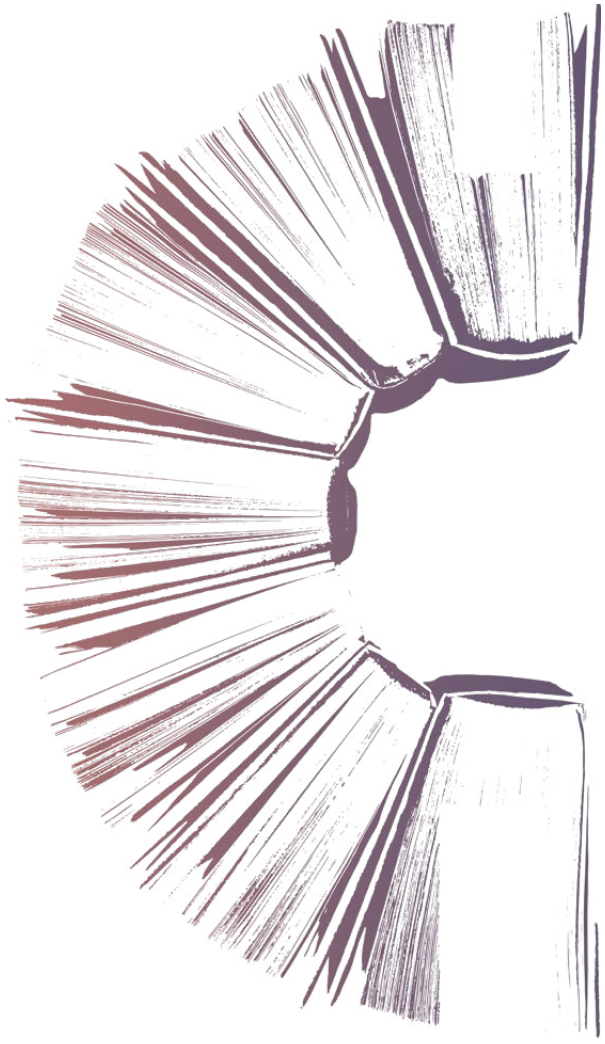
It should be noted that not all collections of personal information are considered personal information banks. The key to determining whether a group of files is a personal information bank is the way it is arranged or retrieved. Consider whether the information organized and capable of being retrieved by a personal identifier.

The PID must include the following information with respect to each personal information bank:

- its title and location
- a description of the kind of personal information and the categories of individuals whose personal information is included
- the authority for collecting the personal information
- the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed
- the categories of persons who use the personal information or to whom it is disclosed

This directory will **not** include the actual personal information collected, only a description of the kind of personal information. For example, a Public Library's Human Resources Office maintains a personal information bank of the Public Library's personnel files. An example PID listing for these files is:

a. **Title:** Personnel Files; Location: Human Resources Office
b. **Personal information:** name, address, social insurance number, marital status, family status, employment history, educational history. Individuals: employees of the Public Library
c. **Authority:** *FOIPPA*, E*mployment Standards Act, Labour Relations Code*, and *Library Act*
d. **Purpose:** to document and manage employment history of Public Library employees
e. **Used by:** Public Library Human Resources, Payroll, Directors, and employee supervisors



11 *FOIPPA* s. 69(6).

COLLECTING PERSONAL INFORMATION

Examples of collection of personal information:

- **contact information** to register a new individual for a Public 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 Public Library facilities
- **event registration** and attendance
- **internal emails**, notes, memos, and messages created by Public Library employees
- Public 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 Public Library property

Public Libraries 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 the Collection Notice (see Collection Notices section below).

Authority for Collecting Personal Information

Public Libraries may only collect personal information as allowed by s. 26 of *FOIPPA*. Some of the most common authorities for collection include:[12]

- the collection of the information is expressly authorized under an Act (s. 26(a)) [for example, the *Library Act* or the *Employment Standards Act*]
- the information is collected for the purposes of law enforcement (s. 26(b))
- the information relates directly to and is necessary for a program or activity of the public body (s. 26(c))
- the information is necessary for the purposes of planning or evaluating a program or activity of a public body (s. 26(e))
- the information is collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appears, and that is open to the public (s. 26(g))

Most of a Public Library's collection will be authorized under s. 26(c) of *FOIPPA*: the collection relates directly to and is necessary for a program or activity of the Public Library. See the discussion below about what information is "necessary".

Public Libraries do **not** have the option of obtaining an individual's **consent** to collect personal information. Consent is not an authority for collection in *FOIPPA*. Below, these guidelines discuss the scenarios where it may be appropriate to obtain an individual's consent to "use" or "disclose" their personal information (such as for a new use or a new or unexpected disclosure for information that has already been collected by the Public Library).

Helpful Tool

See the **template and sample Collection Notice** in the Resources section at the end of these guidelines.

12 *FOIPPA* s. 26 for a full list of authorized collection purposes.

Source of Personal Information

Public Libraries must, with limited exceptions, collect personal information directly from the person to whom it pertains.[13]

Public Libraries may only **indirectly** collect personal information about an individual from another source under the circumstances set out in *FOIPPA* s. 27(1), including if the indirect collection is authorized by the individual the information is about or an enactment (27)(1)(a)), or if the indirect collection is for the purposes of debt collection or law enforcement(27(1)(c)).

Collection Notices

When collecting personal information, Public Libraries must provide the individual with a Collection Notice. The Public Library must ensure that an individual from whom it collects personal information is told:

- the **purpose** for collecting it.
- the **legal authority** for collecting it.
- the **contact information** of an officer or employee of the Public Library who can answer the individual's questions about the collection.

Collection notices should be presented before or at the time of collection. Best practice is that Collection notices are presented in writing, but the notice may be spoken to the individual when collecting information over the phone. Further guidance on collection notices is available through the BC Government.

Limiting Collection to What is "Necessary"

Most of a Public Library's collection will be authorized under s. 26(c) of *FOIPPA*: the collection relates directly to and is necessary for a program or activity of the Public Library. For collection under this authority, Public Libraries must limit the collection to what is "necessary". Personal information should not be collected indiscriminately.

Making a necessity determination can be complex. According to the OIPC, "necessary" does not mean impossible to operate without. Consider whether there are reasonable alternatives to avoid collecting the personal information. More sensitive personal information will have a higher necessity threshold.

For example, when registering a new patron, Public Libraries typically collect the individual's phone number for the purposes of identifying and contacting that individual. While it is certainly possible that patron registration could take place without collecting a phone number, it serves a reasonably important purpose and is not sensitive personal information in this context. Unnecessary personal information for registration would include details such as reading preferences, preferred media format, level of computer skills, or languages spoken. On the other hand, if the collection is for a recommendation service that members can opt-in to, necessary collection for that service may be details such as reading preferences, preferred media format, and languages spoken.

AVOID COLLECTING INFORMATION WHEN ONLY SEEKING TO VERIFY

Most Public Libraries require individuals to show identification showing their name and home address. Consider whether retaining a copy of this ID, or recording an ID number, is necessary. Instead, a library could simply document that ID was checked using a checkbox on the form or in the system. It may be helpful, especially for new employees and volunteers, to avoid providing any space on the form that may look like it is intended for recording an ID number, or to expressly state on the form that ID numbers should not be noted. Not only does this avoid over-collection or unnecessary collection, but this reduces the risks of harms to individuals in the event of a privacy breach.

13 *FOIPPA* s. 27.

Anonymous Information

When information is collected that cannot be tagged to an identifiable individual, that collection is not "personal information" under *FOIPPA*.

De-identified information, which may be re-identified (for example, through a key), is not truly anonymous, and is still within the scope of *FOIPPA*.

In smaller communities, anonymous information could still inadvertently identify an individual. For example, there may be only one man in town who is over the age of 70 and whose preferred language is Hungarian. Because the individual may easily be identified through the mosaic effect, this constitutes personal information and needs to be protected under *FOIPPA*. A best practice would be to review information that is intended to be anonymous and remove potential identifiers from reports or compilations.

When Personal Information is Not Collected

Personal information that is unexpectedly received by a Public Library is not "collected" by the Public Library for the purposes of *FOIPPA* if:

- the information does not relate to a program or activity of the Public Library; and
- the Public Library takes no action with respect to the information other than to read all or a part of it and then delete, destroy, or return it.[14]

This section is important in the event that the Public Library receives personal information that it does not intend to collect (see the Authority for Collecting Personal Information section above), as the unauthorized collection of personal information is a breach of *FOIPPA*.[15]

14 *FOIPPA* s. 27.1(1).
15 *FOIPPA* s. 25.1.

PERSONAL INFORMATION OF CHILDREN / MINORS

Minors Under 12 Years Old

Under s. 76(1) of the *Child, Family and Community Service Act*, [RSBC 1996] c. 46, a person who has legal care of a **child under 12 years of age** (i.e., ages 0 to 11) may, on behalf of the child, exercise the child's following rights under *FOIPPA*:

- to be given access to information about the child in a record
- to consent to the disclosure of that information
- to request the correction of that information

NOTE: A MINOR'S AGE IS DETERMINED AS OF THEIR EXACT BIRTHDAY (NOT GROUPED BY CALENDAR YEAR).

Capacity to Act Under *FOIPPA*

Under s. 3 of the *FOIPPA* Regulation[16] , guardians may act for a minor with respect to the following provisions of *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

Acting "for" a minor child in exercising the child's rights means acting to benefit the child, to further the child's own goals or objectives in the child's best interests.

Minors have the rights of individuals under *FOIPPA* unless the minor is "incapable" of exercising their rights under *FOIPPA*. 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, even when in contradiction to what their parents or guardians might want for them.

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*. Capacity should be determined with a consideration of the potential risks, harms, and implications related to the provision in question, with a respect for the minor's personal autonomy, and by interacting with the minor and asking them questions to gauge their level of understanding.

Public Libraries 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. The Public Library's policy on children should not be applied so rigidly that such a child is not able to exercise their rights under *FOIPPA*.

Library Card Registration of Minors

Public Libraries may choose to only allow minors to hold Public Library accounts if an adult co-signs to accept responsibility for the activities on that account, such as incurred fees and fines. In this case, capable minors should be informed at the time of account creation, and ideally through information posed at the Public Library or online, that their account personal information will be disclosable to their guardian until they reach the age of 19. Procedures should be put into place to update accounts when capable minors reach the age of 19.

16 B.C. Reg. 155/2012.

Disclosing Personal Information of Minors

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.

Public Libraries may disclose personal information if the head of the Public Library determines that compelling circumstances that affect anyone's health or safety exists *(FOIPPA s.33(3)(a))*. This disclosure could be to anyone necessary, including law enforcement, medical professionals, or parents/guardians.

Note that the head of the Public Library, 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 Public 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 Public 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.

THEN: The Public Library should verify the guardian's identity: if by phone, with tow or three verifying questions using the information recorded on the file; and if in person, by checking ID.

Once identification is verified, the Public Library 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.

THEN: 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 Public Library should inform the guardian that because they are not named on the account, the Public Library cannot disclose the personal information. The Public 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 Public Library should seek proof of guardianship and verify the identity before disclosing information.

ACCURACY AND CORRECTION

Accuracy of Personal Information

The Public Library 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 Public Library's custody or control that is used by the Public Library to make a decision that directly affects the individual.[17]

For example, if a certain age limit is required to receive a benefit or attend an activity, the Public Library should verify the individual's age by viewing government-issued identification.

'Reasonable efforts' to ensure accuracy may include:

- verifying possibly outdated information
- periodic checks, directly with the individual the information is about or using other authorized avenues, to ensure the information is still current and valid
- thorough reviews of applications to ensure all questions are answered completely (e.g., applications for employment)
- documenting when personal information is collected or received
- documenting how personal information has been verified
- having a process in place for an individual to correct or request a correction to their personal information

Correction of Personal Information

Upon request by an individual, the head of a Public Library is required to correct (or note requested corrections to) inaccurate or incomplete personal information in its custody or control.

An individual who believes there is an error or omission in their personal information that is in the custody or under the control of the Public Library may request the head of the Public Library correct the information[18].

If no correction is made in response to a request, the Public Library must annotate the information with the correction that was requested but not made.

On correcting or annotating personal information, the Public Library must notify any other third party to whom that information has been disclosed during the one-year period before the correction was requested.

Individuals should be able to provide proof that information is wrong or incomplete in order for a correction to be made. Opinions and other types of subjective information do not lend themselves to correction in most cases. For those requests, an annotation may be more appropriate than a correction.

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

The best approach is to implement procedures about how correction requests should be handled. This promotes consistency, quality, and timeliness in decision-making.

17 *FOIPPA* s. 28.

18 *FOIPPA* s. 29.

USE OF PERSONAL INFORMATION

Personal information in the custody or control of the Public Library must not be "used" by the Public Library (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*.

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 purpose19
- if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or
- for a purpose for which that information may be disclosed to that Public Library under s. 33.

When considering using previously collected personal information, Public Libraries must consider whether the proposed new use meets one of the three criteria established in s. 32. Any use not meeting one of the three criteria is not permitted under *FOIPPA*.

Consent for Use

Consent for the use of personal information must be obtained when the Public Library 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.[20]

The required elements of consent for use are set out in s. 11 of the *FOIPPA* Regulation.[21] Consent for 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

Note that consent for **disclosure** has different requirements. See the **Disclosure of Personal Information** section below.

Consent by an individual must be freely given and optional. An individual must understand their right to refuse to provide consent. To help ensure consent if voluntary, consider having an opt-out process and an alternative process should an individual not consent.[22]

See the template consent form in the *Resources* section at the end of this document.

Consistent Purpose

Some uses may be for a "consistent purpose" for which the personal information was obtained. A use for a "consistent purpose" is if the use:

- has a reasonable and direct connection to that purpose; and
- is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.[23]

Public Libraries should consider whether the person the information is about would expect their information to be used in the proposed way. Public Libraries must ensure that a consistent use has a logical and plausible link to the original purpose for which the personal information was obtained or compiled. It should flow or be derived directly from the original use or be a logical outgrowth of the original use.

19 For the definition of a "consistent purpose", see *FOIPPA* s. 34.
20 a public body does not have to seek consent for a use for a different purpose if that use is for a purpose authorized under s. 32(c) - i.e., any purpose for which a public body can disclose personal information under s. 33(2).
21 B.C. Reg. 155/2012.
22 If an individual doesn't consent to the use, the public body can either not use the personal information or provide the alternate (e.g., using a manual process to sign someone up for a library card rather than an online application).
23 *FOIPPA* s. 34.

SECURITY OF PERSONAL INFORMATION

A Public Library must protect the personal information it holds by making "reasonable security arrangements" against such risks as unauthorized access, collection, use, disclosure or disposal.[24] Security arrangements can be administrative/procedural, physical, or technical, and apply to prevent breaches both from within and from outside of the Public Library.

What is considered "reasonable" for a security arrangement depends on factors such as the sensitivity of the information, foreseeable risks, likelihood of harms or damage, the medium/format of the record, and industry standards.

Helpful Tool

The Public Library may work with its IT personnel to review the security arrangements using the OIPC's **"Securing Personal Information – A self-assessment tool for public bodies"** checklist, available online in the OIPC guidance documents.[25]

Three Types of Security Controls: Administrative, Physical and Technical

ADMINISTRATIVE SECURITY MEASURES ACCESS RESTRICTIONS

Public Libraries should implement role-based access to technology resources as a type of 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 should be documented, remain up-to-date and be assigned on a consistent basis.

- **Need-to-know** - Access is restricted to only those employees who require access to carry out their work. The need-to-know principle may be implemented in various ways, such as:
  - physically segregating and controlling access to certain records
  - physically segregating and controlling access to certain records
  - listing individuals who may access certain records installing technical access controls on information systems

EXAMPLES OF RESTRICTING ACCESS ON A NEED-TO-KNOW BASIS

- **Patron name, barcode, contact information** - only employees or volunteers who check out materials, update personal information or place holds for patrons (e.g., Circulation and Reference staff).
- **Patron borrowing history** - only employees or volunteers who assist patrons to access this 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.
- **Employee timesheets** - only employees or volunteers responsible for supervising employees and volunteers or payroll.
- **Employee criminal record check reports** - only employees or volunteers responsible for screening employees in this regard (e.g., Human Resources Director, Chief Librarian or Board members).

24 *FOIPPA* s. 30.

25 Dated October 2020, accessible through the OIPC Guidance Documents, at https://www.oipc.bc.ca/guidance-documents/1439.

- **Least privilege** - Access is restricted to only that information which an employee needs to carry out their work. The intention of this principle is to limit the damage that can result from accidental or unauthorized use. Employees are not entitled to access information merely because of status, length of service, rank, or office.[26]

System logs, if practical, should be audited periodically to ensure that users are accessing information appropriately. Managed access control lists are ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information, or track who has access to files containing sensitive information.

TRAINING AND AWARENESS FOR EMPLOYEES/VOLUNTEERS

Training is very important and can be considered an **Administrative Control.** A lack of privacy training and awareness can result in a privacy breach (such as misdirected email or inappropriate records disposal). Only employees and volunteers who are fully aware of the requirements for protecting personal information should be authorized to begin handling personal information.

Each employee and volunteer should know the contact information for the Public Library's Privacy Officer and be informed of privacy policies and procedures, including how and when to report a privacy breach to the Public Library. This document may help by being a part of the "action plan", enabling employees and volunteers to be aware of and ready to act upon privacy issues as they arise.

Privacy training is not just for new employees. It is a best practice for existing employees to refresh their privacy training and review requirements regularly.

Helpful Tool

In addition to job-specific privacy training, the BC Government offers a free online *FOIPPA* privacy training course for BC public body employees and service providers: ***FOIPPA* Foundations: https://mytrainingbc.ca/FOIPPA/.** The course should take about 60 to 90 minutes to complete.

CONFIDENTIALITY AGREEMENTS

Public Libraries should have confidentiality agreements with employees and volunteers who are authorized to access personal information. The confidentiality agreements should stipulate that the employee/volunteer will comply with the requirements of FOIPPA and the Public Library's privacy policies when dealing in any way with personal information and stipulate what steps may be taken to enforce the policies.

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. See the section below on service providers and contracts.

Where contracted services are used for storage, transportation or destruction of records, Public Libraries should require the contractors to provide a certificate of destruction.

PHYSICAL SECURITY MEASURES

Some examples of physical security measures are:

- storing records containing personal information in locked storage rooms or locked filing cabinets, with controls over distribution of keys or lock combinations;
- methods to label file drawers, records storage boxes and other storage containers so employees only access the records they need to access; or
- positioning of computer screens so they are not visible to others.

26 This includes board members and local government officials.

VIDEO SURVEILLANCE

The OIPC (BC) has published guidance documents outlining how *FOIPPA* applies to the use of video and audio surveillance systems by public bodies. Please use these documents as the guide:

- OIPC, BC - Using Overt Video Surveillance (2017)
  If collecting personal information via video surveillance is necessary and authorized under the legislation, you will need to develop appropriate policies and procedures. The video surveillance policy should explain the rationale and purpose of the surveillance; when and how monitoring and/or recording will be in effect; how recordings will be used; for how long they will be kept; how they will be securely deleted; and a process to follow if there is unauthorized access or disclosure.
- OIPC, BC - Public Sector Surveillance Guidelines (2014)
  Section 27(2) of *FOIPPA* requires that public bodies notify individuals when they are collecting personal information. A Public Library should notify the public, using clearly written signs prominently displayed at the perimeter of surveillance areas so the public has sufficient warning that video or audio surveillance is or may be in operation before entering any area under surveillance. The notification must state: the purpose for the collection, the legal authority for the collection, and the title, business address and business telephone number of an employee of the Public Library who can answer the individual's questions about the collection.

TECHNICAL SECURITY MEASURES

Each Public Library should ensure that their internal or contracted IT personnel are aware of the Public Library's legal duty to protect and secure records containing personal information. Where possible, work with qualified technology professionals experienced at protecting data in systems.

Some examples of technical security measures are:

- encryption of files in transit or at rest
- encryption of files containing personal information that will be sent over e-mail
- firewalls, intrusion detection, malware, etc.
- role-based access controls
- access logs
- encryption, firewalls, VPNs
- two-factor Authentication
- automatic log-outs and screen locks

RETENTION AND DISPOSAL OF PERSONAL INFORMATION

A Public Library must retain personal information for at least one year after it is used to **make a decision that directly affects the individual that the information is about.**[27]

There are no other retention limits specified in *FOIPPA*, but other laws may apply to the personal information to dictate retention periods (e.g., employee pay records).

To minimize the risks of unauthorized use and disclosure of personal information in the Public Library's custody or control, **a Public Library should not retain personal information that is no longer required** for operational, legal or archival reasons. Public Library policies should guide staff in applying an appropriate retention period to categories of records.

Policies should also specify the appropriate and secure method of disposal of personal information, both in hardcopy and electronic form.

TIPS ON DESTROYING PERSONAL INFORMATION:

- **Paper:** Should be shredded (ideally using a cross-shredder), burned or pulped. Never throw paper with personal information into a recycle bin unless it is in a secure location and stays secure until it is shredded.
- **Electronic data:** Computer files are not destroyed simply by "deleting" the file from the computer's recycles bin. Deleting merely removes the file name from the directory and allows the data to be overwritten eventually. Data must be purposefully overwritten, "wiped", or "sanitized". Even emails that are double-deleted (deleted from the inbox and then deleted from the trash folder) may be accessible on server backups. Seek assistance from an IT professional to develop procedures for data erasure.

27 *FOIPPA* s. 31.

Internet Search History Logs and Lendable Tech

Public Libraries should set up automatic purging of the cache and history folders on public access computers after each user session.

Information saved on lendable tech must be permanently cleared before circulating to the next patron. Similarly, procedures need to be followed to permanently remove information from electronic devices before disposal; simply deleting the data on these devices will not necessarily prevent its recovery.

DISCLOSURE OF PERSONAL INFORMATION

Public Libraries may only disclose personal information for the purposes set out in *FOIPPA* s. 33. Some of the more 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 the Public Library 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 the Public Library or the government, or for the purposes of **a payment to be made** to or by the Public Library or the government (e.g., debt)
- to a public body or **law enforcement agency** in Canada, to assist in a specific investigation
- the head of the Public Library determines that **compelling circumstances** that affect anyone's **health or safety** exist
- for a **research** purpose under a research agreement
- in accordance with a**n 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 the Public Library, some of the purposes may entail a mandatory disclosure (for example, to comply with a court order).

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.

Consent for "use" of personal information has different requirements- see the "Use of Personal Information" section above.

28 B.C. Reg. 155/2012

Disclosures in Practice

The following are example situations where disclosing information is appropriate:

If

The Public Library has a good relationship with the local police, who routinely ask for information about individuals.

THEN: To provide personal information to police, there must be a specific investigation underway. Casual disclosures are not authorized.

If

A patron provides consent for his sister to pick up materials on his behalf, for the purpose of delivering the materials to him.

THEN: If proper consent in the prescribed form is obtained, the Public Library may disclose the materials. For ongoing pick-up of materials, the Public Library may wish to make a note on the patron's file.

If

The Public Library is trying to collect a debt owed by the individual the personal information is about.

THEN: The Public Library may disclose a patron's personal information to whoever necessary in order to collect a debt, receive or make a payment.

If

The Public Library initiated contact with the police about an incident that occurred or is occurring in or around the Public Library.

THEN: The Public Library may disclose personal information to the police to open an investigation into the incident.

If

The police or the CRA are requesting information about an individual, related to an active investigation file that has nothing to do with the Public Library.

OR

The police are requesting video footage of an individual relating to an incident occurring in or around the Public Library.

THEN: 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.

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.

If

An individual has been disruptive or breached the Public Library's rules.

THEN: The Public Library 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).

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).

If

The head of the Public Library, or its delegate, believes there are compelling circumstances that affect someone's health or safety.

THEN: The Public Library may disclose an individual's personal information in these circumstances to whoever necessary, including the individual's family members, law enforcement, or medical personnel.

FREEDOM OF INFORMATION (FOI) ACCESS REQUESTS

The public has a right of access to all records in the custody or under the control of the Public Library, subject to some 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 Public Library's 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 the Public Library such as copies of contracts or internal communications.

Records that are exempt from FOI Access Requests include:[29]

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

The Public Library 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*).

Public Libraries should confirm an individual's identity before providing records about that individual.

Fees for Accessing a Record

Public Libraries may charge an applicant a prescribed application fee for FOI Access Requests, unless the request is for an individual's own personal information. At the time these guidelines are written, the prescribed fee is $10.[30]

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:[31]

- 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.

29 *FOIPPA* s.3(5).
30 *FOIPPA* Regulations. 13(2).
31 *FOIPPA* s. 75.

Public Libraries must 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 head of the Public Library. Applicants may provide a written request to excuse payment of all or part of the fees. The head of the public body may excuse payment, if, in the head of the public body's opinion,

a. the applicant cannot afford the payment or for any other reason it is fair to excuse payment, or
b. the record relates to a matter of public interest, including the environment or public health or safety.

PRIVACY BREACHES AND COMPLAINTS

Privacy and Access Complaints

Public Libraries should be prepared to address an individual's challenge concerning the Public Library's privacy or access compliance with *FOIPPA*.

Privacy complaints may include:

- 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.

FOI Access complaints may include:

- 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.

The OIPC's directions to individuals[32] who wish to make a privacy complaint are as follows:

1. The first step is to attempt to resolve your complaint directly with the public body or organization. Submit your complaint in writing directly to the public body or to an organization's privacy officer. Provide as much detail as you can to assist them to understand the nature of your complaint. Ask the public body or organization to explain their legal authority to do what they did.
2. Give the public body or organization at least 30 business days to respond. We generally do not accept complaints until you have waited at least 30 business days for a response. Keep copies of your correspondence with the public body or organization as we will need to see them.
3. If after 30 business days, you have not received a response from the public body or organization you can make a complaint to our office.
4. Or, if you are unsatisfied with how the public body or organization addressed your complaint, you can make a complaint to our office.

If the Public Library receives a privacy complaint about how an individual's personal information has been handled by the Public Library, consult the individual responsible for privacy in the Public Library about next steps. You can also ask the OIPC to provide guidance in response to a complaint. You may be able to demonstrate to the individual that policies, procedures, or guidelines were followed, and show that collection, use, or disclosure was authorized.

If the Public Library is unable to resolve the complaint with the individual directly, 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 the Public Library complied with *FOIPPA*.

32 How do I make a complaint? - Office of the Information and Privacy Commissioner for BC (oipc.bc.ca)

Privacy Breaches

Mandatory Breach Notifications - **Section 36.3** requires the head of a public body to 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 section **36.3.** The head is also required to notify the Information and Privacy Commissioner (the Commissioner) when the significant harm threshold is met.

Guidance on Mandatory Privacy Breach Notifications is available on the BC Government website.

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of *FOIPPA*.

The most common privacy breaches happen when personal information of patrons or employees is stolen, lost, or mistakenly disclosed (e.g., when a computer is stolen or when personal information is mistakenly emailed to the wrong person).

Privacy breaches can cause significant harm to individuals. For example, an individual whose privacy has been breached may be at risk of identity theft, physical harm, humiliation, and damage to personal or professional reputations, or loss of business or employment opportunities.

REPORTING PRIVACY BREACHES TO THE PUBLIC LIBRARY

Reporting mechanisms should be established within the Public Library for employees and the public to report privacy breaches to the Public Library. Those employees who report internal privacy breaches to the Public Library should be protected under policy (e.g., a whistleblower provision). Employees should be made aware of their duty under *FOIPPA* to report privacy breaches:

> ***FOIPPA s. 30.5(2): An employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the head of the public body.***

PROCEDURES FOR RESPONDING TO PRIVACY BREACHES

FOIPPA, Section 36.2 - requires B.C. public bodies to develop a Privacy Management Program (PMP), including the requirement for a breach process. A PMP is an evolving set of policies, procedures and tools developed by a public body to enable systematic privacy protection throughout the personal information lifecycle. **Guidance is available from the BC Government website.**

Procedures should be developed for how the Public Library responds to actual or potential privacy breaches. Steps may include:

1. Identify and contain the breach
2. Report the breach to the appropriate people at the Public Library
3. Consider notification to affected individuals
4. Investigate the circumstances around the breach
5. Develop mitigation strategies to avoid the breach in the future

Steps taken should be documented by the Public Library. Privacy breaches may result in civil lawsuits or complaints to the OIPC that are investigated by the OIPC.

In developing response procedures, Public Libraries should consult the OIPC (BC) Guide Document: Privacy Breaches: Tools and Resources, which contains a Privacy Breach Checklist and information on how and when to notify affected individuals (for example, if it is necessary to avoid or mitigate harm to the individual).

REPORTING A PRIVACY BREACH TO THE OIPC

With the legislative changes to *FOIPPA* in November 2021, a new provision was added that came into force February 1, 2023. Section 36.3 of *FOIPPA* requires each public body to:

- notify affected individuals if the privacy breach could reasonably be expected to result in significant harm to the individual; and
- notify the commissioner of the OIPC if the breach could reasonably be expected to result in significant harm to an individual.

Helpful Tool

More information on how the OIPC helps public bodies after breach notification is available here: **www.oipc.bc.ca/resources/report-a-privacy-breach**

PRIVACY IMPACT ASSESSMENTS

Public Libraries are required to conduct a Privacy Impact Assessment ("PIA") in accordance with the Minister of Citizen's Services Directions for all new initiatives or before any significant change to an initiative of the Public Library.[33]

Effective November 26, 2021, the Minister's Directions for conducting PIAs are set out in Direction 2-21. The BC Government offers a template PIA form for non-ministry public bodies, available online.[34] The template will navigate the Public Library through the Minister's Directions, which is a series of questions that must be answered about the initiative.

What is an Initiative?

Initiatives include:

- any enactment, system, project, program, or activity. This includes any time the Public Library is contracting with a new service provider, hosting a new program, or setting up a new system.

For example, if a Public Library is considering implementing the Square payment system or Moneris payment system, a PIA should be conducted for the product under consideration.

PIAs must be conducted for all initiatives, which even extends to include initiatives that do not collect or use personal information. For initiatives that do not collect or use personal information, the PIA questions are fewer, and involves asking how the Public Library will reduce the risk of unintentionally collecting personal information through the initiative.[35]

The Purpose and Elements of a PIA

The purpose of the PIA is to:

a. Determine whether the initiative meets or will meet the requirements under Part 3 – '*Protection of Privacy*' of *FOIPPA*; and
b. Identify and assess privacy risks and identify a risk response(s) (i.e., mitigation strategy) that is proportionate to the level of the risk.

A PIA involves documenting and reviewing all potential implications of the Public Library's proposed program or activity involving collection, use and disclosure of personal information, and planning in advance to ensure that the Public Library's obligations under *FOIPPA* are met and that privacy rights and interests of individuals are adequately considered and accommodated throughout the program or activity.

An example 'privacy risk' is that the initiative results in the retention of personal information longer than is necessary, which increases the risk of unauthorized use, access, and disclosure. An example 'risk response', or mitigation strategy, is for the Public Library to create a retention and destruction schedule for the personal information.

The 2021 PIA Directions have been amended from the previous Minister's Directions, and now includes the requirement that the Public Library designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative. Accountability may fall to senior managers overseeing the initiative, while the Public Library's Chief Librarian or Director may be the appropriate position for higher risk initiatives.

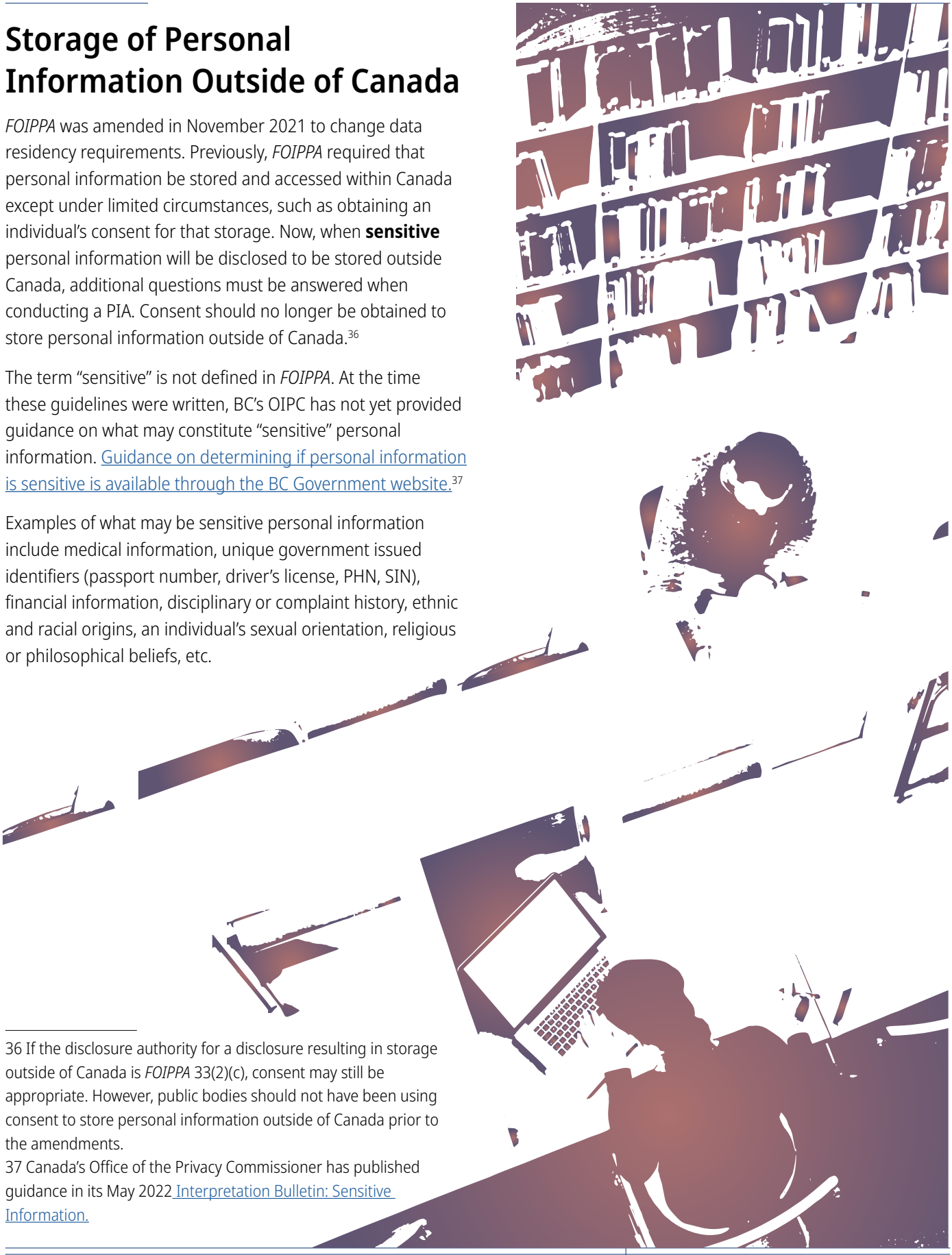
33 *FOIPPA* s. 69(5.3).
34 "PIA template for non-ministry public bodies" available at: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments/complete-a-privacy-impact-assessment#step-one.
35 BC Government PIA template for non-ministry public bodies, question 4.

Storage of Personal Information Outside of Canada

FOIPPA was amended in November 2021 to change data residency requirements. Previously, *FOIPPA* required that personal information be stored and accessed within Canada except under limited circumstances, such as obtaining an individual's consent for that storage. Now, when **sensitive** personal information will be disclosed to be stored outside Canada, additional questions must be answered when conducting a PIA. Consent should no longer be obtained to store personal information outside of Canada.[36]

The term "sensitive" is not defined in *FOIPPA*. At the time these guidelines were written, BC's OIPC has not yet provided guidance on what may constitute "sensitive" personal information. Guidance on determining if personal information is sensitive is available through the BC Government website.[37]

Examples of what may be sensitive personal information include medical information, unique government issued identifiers (passport number, driver's license, PHN, SIN), financial information, disciplinary or complaint history, ethnic and racial origins, an individual's sexual orientation, religious or philosophical beliefs, etc.



36 If the disclosure authority for a disclosure resulting in storage outside of Canada is *FOIPPA* 33(2)(c), consent may still be appropriate. However, public bodies should not have been using consent to store personal information outside of Canada prior to the amendments.

37 Canada's Office of the Privacy Commissioner has published guidance in its May 2022 Interpretation Bulletin: Sensitive Information.

SERVICE PROVIDERS (OUTSIDE CONTRACTORS)

When an outside business or organization is used to provide services on behalf of the Public Library, under *FOIPPA*, it is as though the Public Library was providing the service itself. In other words, the Public Library is responsible for how the service provider deals with personal information in the course of providing services for the Public Library.[38] It is important for the Public Library to know exactly how personal information will be treated in every aspect of the service provided.

Service providers include:

- website developers, cataloguing programs (e.g., SaaS, IaaS, PaaS), Zoom, Eventbrite, accessibility software, HR and payroll software, etc.

Contractual Language

A tool for ensuring service providers understand and agree to their obligations under *FOIPPA* is to append a Privacy Protection Schedule ("PPS") to a contract with a service provider if the service involves personal information. The BC Government's PPS templates are available online through their website.[39] If the contract involves **cloud** services and personal information, the privacy protection schedule for cloud services is more appropriate.

If a PPS is not appended, seek to include clear contractual requirements, including:

- the service provider's acknowledgement that it is a service provider to the Public Library subject to *FOIPPA*
- the service provider will limit the collection, use and disclosure of personal information to specified contractual purposes
- the service provider will implement reasonable security arrangements to protect personal information
- the service provider will comply with privacy policies and controls of the Public Library, including with respect to storage, retention, and secure disposal of records
- the service provider will notify the Public Library in the event of a privacy breach

There may be times that the Public Library uses a service provider who will not engage in contractual negotiations and requires the acceptance of their standard Terms of Service or End-User License Agreement. The Public Library should review the terms of the agreement and the privacy policies of the service provider, ask any outstanding questions to the service provider's privacy contact, and assess the privacy risks of the initiative through the Privacy Impact Assessment process.

Despite contractual language to the contrary, *FOIPPA* applies and prevails. Public Libraries cannot contract out of the law.

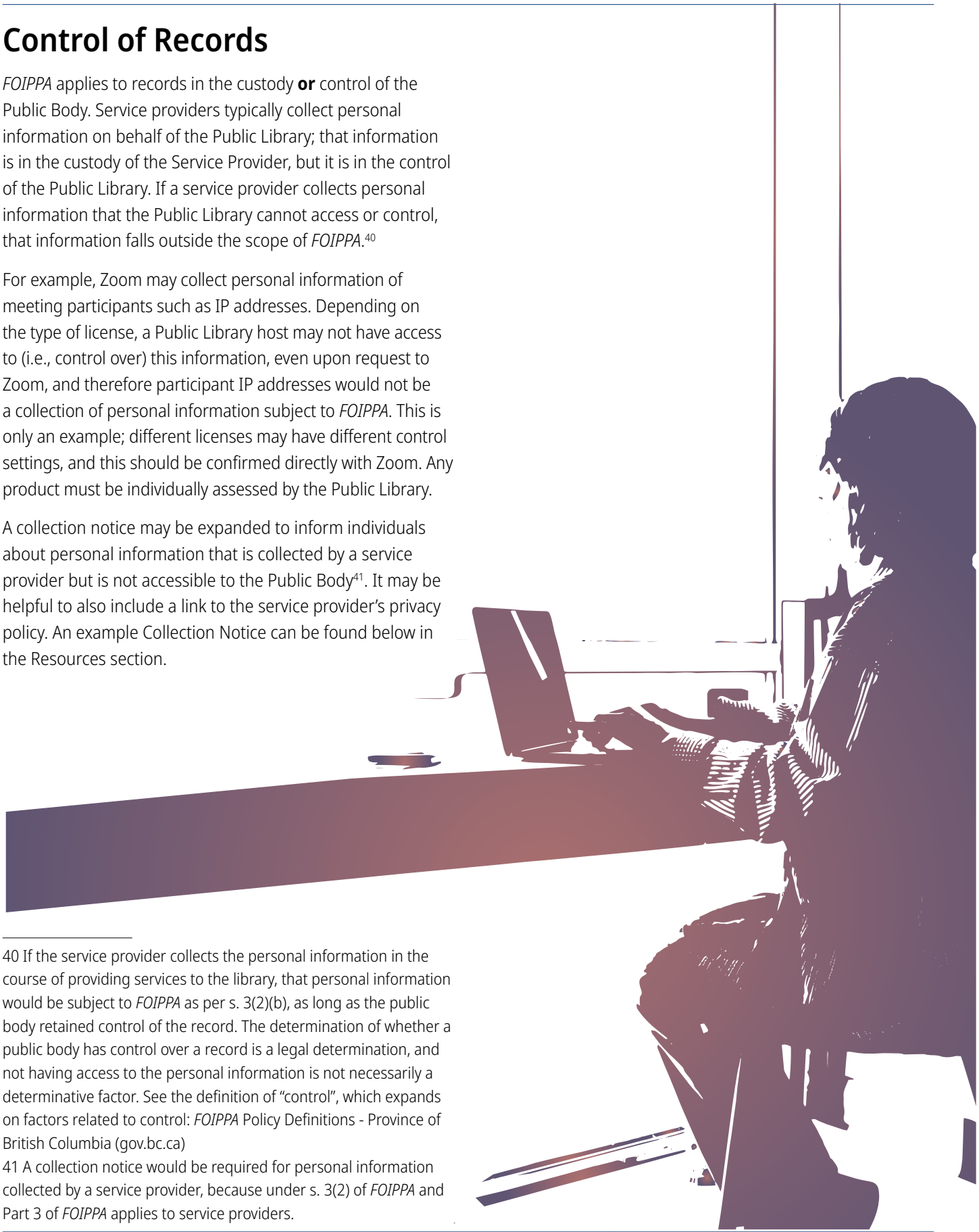
38 See *FOIPPA* s.3(2) and Schedule 1 definitions of 'employee' and 'service provider'.
39 https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/privacy-protection-schedule

Control of Records

FOIPPA applies to records in the custody **or** control of the Public Body. Service providers typically collect personal information on behalf of the Public Library; that information is in the custody of the Service Provider, but it is in the control of the Public Library. If a service provider collects personal information that the Public Library cannot access or control, that information falls outside the scope of *FOIPPA*.[40]

For example, Zoom may collect personal information of meeting participants such as IP addresses. Depending on the type of license, a Public Library host may not have access to (i.e., control over) this information, even upon request to Zoom, and therefore participant IP addresses would not be a collection of personal information subject to *FOIPPA*. This is only an example; different licenses may have different control settings, and this should be confirmed directly with Zoom. Any product must be individually assessed by the Public Library.

A collection notice may be expanded to inform individuals about personal information that is collected by a service provider but is not accessible to the Public Body[41]. It may be helpful to also include a link to the service provider's privacy policy. An example Collection Notice can be found below in the Resources section.



40 If the service provider collects the personal information in the course of providing services to the library, that personal information would be subject to *FOIPPA* as per s. 3(2)(b), as long as the public body retained control of the record. The determination of whether a public body has control over a record is a legal determination, and not having access to the personal information is not necessarily a determinative factor. See the definition of "control", which expands on factors related to control: *FOIPPA* Policy Definitions - Province of British Columbia (gov.bc.ca)

41 A collection notice would be required for personal information collected by a service provider, because under s. 3(2) of *FOIPPA* and Part 3 of *FOIPPA* applies to service providers.

PRIVACY IN PRACTICE

Video Conferencing and Virtual Programing

Many Public Libraries make use of video conferencing tools such as Zoom and offer virtual online programming. Even if a session is not recorded by the Public Library, the service provider may be collecting personal information from attendees. Depending on the service provider used, the personal information that may be collected during these sessions includes:

- display name, which may include a first and last name if the attendee chooses to enter them
- information about an attendee's device, network, and internet connection (e.g., IP address(es), MAC address, device type, operating system, and client version)
- information about an attendee's usage of or the interaction with the service provider's products
- other information an attendee uploads, provides, or creates while attending a session
- if recorded, an attendee's image, voice, name, or personal views and opinions

Conducting a Privacy Impact Assessment will help the Public Library determine what personal information is collected by a video conferencing tool and whether that activity is authorized by *FOIPPA*.

Individuals must be provided with a Collection Notice setting out what personal information is being collected by the service provider. See the Collection Notice section above, and the Collection Notice template and samples in the Resources section, below. Consent should not be obtained for the collection of personal information through video conferencing, as consent is not a proper authority for collection (see the Collection section, above).[42]

The Public Library should avoid unnecessarily retaining a recording of virtual sessions. If retaining a recording, identify an authorized purpose for that collection and ensure all attendees are informed that the session will be recorded.

Practices you may wish to implement to increase privacy include:

- allowing users to join sessions anonymously
- locking or password protecting sessions from general public access (e.g., for employee meetings)
- retaining the ability to expel participants from a session
- making use of a 'waiting room' feature that allows the host to admit specific individuals
- restricting the ability for hosts or users to record sessions

Debt Collection

Public Libraries that have difficulties with unreturned materials may choose to collect certain personal information (such as ID numbers or references) specifically for the purpose of debt collection, directly or indirectly. Public Libraries may disclose personal information without consent for the purpose of collecting a debt owed to them. Disclosure could be to whoever necessary, including law enforcement, parents/guardians, and collection agencies. However, disclosure should be limited to personal information that is reasonably necessary to collect the debt.

A Public Library may also ask other Public Libraries for personal information about a patron for the purpose of collecting a debt owed by that individual as a result of not returning a resource. Indirect collection and disclosure between Public Libraries for this purpose is authorized by s.33(2)(o) and 27(1)(c)(iii) of *FOIPPA*.

NOTE:

Beware of the autofill function. Reconfirm the correct email address has been entered in the 'to' field.

42 A collection notice would likely be required for this collection unless the personal information fell under an exception in *FOIPPA*, s. 27(3). For example, if and individual's name and image of their face were collected by observation at a Zoom event open to the public, this could fall under s. 27(3)(d). That same authority would likely not work for the collection of IP addresses, however, as those are not readily observed. All of these authorities would need to be assessed when evaluating the product/program through a Privacy Impact Assessment.

Patron Registration

Personal information collected from an individual upon their registration with a Public Library should be limited to information that is necessary for the Public Library to offer its services and operate its programs. For example, if knowing the first language of a patron is not necessary, it should not be collected.

If proof of address or identification is required to register an individual, that information may be viewed, rather than copied and retained. Viewing the information is not a "collection" by the Public Library. If a Public Library wants to document that ID was checked, a checkbox on the paper form or a flag in the computer system is sufficient. It may be helpful, especially for new employees and volunteers, to avoid providing any space on the form that may look like it is intended for recording an ID number.

Ensure registration forms contain a Collection Notice on the form.

Internet/Computer Use by Patrons

Ensure a Collection Notice is provided to patrons using Public Library computers, informing them of what personal information is collected (if that information can somehow be associated with the individual). The Collection Notice should be placed where it can be easily noticed and where the individual can read it before using the computer.

Measures to ensure users cannot save personal information on computers to be accessed by the next user should be implemented.

Emailing Personal Information

Where personal information is communicated electronically and could be intercepted by a third party, the communication should be secure (e.g., encrypted). If this is not feasible, then notice should be given that the communication is not protected and may be intercepted by a third party. It's best to think of email as a postcard. When you send a postcard, any number of human mail handlers, automated OCR readers, etc. along the way can see what is written on the back.

The postcard could accidentally be addressed to the wrong individual. Public Libraries should not send sensitive personal information of individuals on the back of postcards, nor should they do so through emails without protections in place (e.g., encrypting attachments).

Ways to protect personal information being transmitted via email include:

- Ensure information is in an encrypted file which is attached to the email, and not in the body of the email itself.
- Do **not** send the document's encryption password to the recipient in the same email as the document. Provide the password by phone or follow-up email.
- Double check that the recipients are authorized to receive the information.

IMPORTANT

Do **not** send any confidential business or sensitive personal information via email unless it is encrypted. Without encryption, the information may be inadvertently sent to the wrong individual(s), and the information may be stored on email servers, increasing the risk of privacy breach.

Reference Questions

Public Libraries provide a valuable service in helping individuals to find information. This is accomplished in a variety of ways, including in person, by email, through the Public Library's own website, or through a third-party service provider. Individuals should have the option of asking references questions anonymously. If personal information is collected (such as IP address, email address, or name), the individual must be provided with a Collection Notice.

Many Public Libraries keep track of questions for follow up, in case they are asked again, or to compile statistical information. Personal information should be removed whenever possible to anonymize this information for compilation.

Marketing and Fundraising

Personal information that the Public Library has collected for another purpose should not be used for marketing or fundraising purposes unless the patron's consent for that use is obtained. Consent can be obtained by providing a box on application/registration forms patrons can check to either "opt-in" or "opt-out" of being contacted for marketing or fundraising purposes.

Every future marketing or fundraising communication sent should include an option to allow patrons to opt-out of those communications.

Employee and Volunteer Personal Information

Employee and volunteer personal information is protected under *FOIPPA*. Records containing personal information about employees and volunteers should be kept secure. Only other employees or volunteers of the Public Library who "need to know" should have access to the information.

Employment history is considered personal information.[43] This refers to any information regarding an individual's work record, such as resumes and references provided, vacation dates, and performance reviews.

Employee and volunteer personal information that is not considered personal information (as defined by *FOIPPA*) includes:

- their business contact information (e.g., work email address and phone number)[44]
- information about their position, functions, or remuneration (e.g., the job classification and exact salary of an employee) [45]

Information about an individual's **"position"** includes that person's job description and classification. Information about an individual's **"functions"** includes a description of duties to be performed in the course of employment.

Information about **"remuneration"** includes salary amount and benefits received as a result of employment. Severance pay is included in the meaning of "remuneration", but this does not include the background personal information used to calculate the severance entitlement, such as age, number of dependents, assessment of the employee's chance of obtaining other employment, etc.

NOTE:

Collection of surveillance and monitoring personal information of employees should be limited to what is necessary, accessible only to those who need to know the information, and individuals must be told (through a Collection Notice) that their personal information is being collected for a certain purpose.

Supervisors may be contacted to provide a reference for a Public Library employee or volunteer. In this case, the supervisor should seek to confirm that the individual has consented to the disclosure of their personal information before providing details about recorded employment history, including the fact that the employee worked at the Public Library and when. A supervisor's unrecorded personal opinions about the employee fall outside of the scope of *FOIPPA*.

43 *FOIPPA* s. 22(3)(d).
44 *FOIPPA* Schedule 1 definitions of "personal information" and "contact information".
45 *FOIPPA* s. 22(4)(e) and s. 33(2)(b).

Surveillance and Monitoring

Employers have the technological ability to continuously monitor their employees as they work, both at home and in the workplace through audio and video monitoring, GPS tracking, and computer software and programs. Public Libraries should beware of over-collection and unauthorized collection, and ensure individuals are provided with appropriate Collection Notices.

The OIPC published a guidance document in November 2017 titled "Employee Privacy Rights",[46] which discusses the privacy impacts of employee monitoring programs. The guidance notes that the collection must be necessary for managing or terminating an employee relationship. Employers must carefully weigh the privacy harm when considering the use of surveillance and monitoring software.

Patrons' Personal Filming and Photography

Individuals attending the Public Library might seek to take photos or videos using their personal devices, for their own purposes. This activity is not a collection of personal information by the Public Library, and those photographs or videos are not records in the custody or control of the Public Library. Therefore, the activity falls outside of the scope of *FOIPPA*.

Public Libraries may either allow this activity or choose to create rules or policies for when photography or filming is permitted on Public Library premises.

Incidents and Rule Breaking

Public Libraries may collect personal information about individuals related to incidents of law or Public Library rule/policy breaking, for the purpose of investigating and enforcing Public Library rules/policies.[47]

This can broadly include names, images, surveillance footage, witness statements, etc.

Public Libraries may also disclose incident personal information to another Public Library or a law enforcement agency in Canada, "to assist in a specific investigation undertaken with a view to a law/rule/policy enforcement proceeding, or from which a law/rule/policy enforcement proceeding is likely to result".[48]

This collection, use, and disclosure can be lawfully done without a collection notice[49] and without the individuals' consent.

Care should be taken by the Public Library to avoid creating or sharing 'black lists' of individuals who 'may' cause future problems for the Public Library. The collection, use, and disclosure are only authorized for **investigations** and **proceedings** that could lead to a penalty or sanction being imposed.

Payment Systems

Some Public Libraries are interested in using the "Square" payment system because it may cost less than the commonly used Moneris system. Implementing a payment system is an "initiative" and therefore it requires a Privacy Impact Assessment (PIA). The third party company, Square, may collect personal information on behalf of the Public Library. The PIA will help the Public Library determine whether the initiative meets the privacy requirements of *FOIPPA*.

46 https://www.oipc.bc.ca/guidance-documents/2098.
47 *FOIPPA* s. 26(b), and Schedule 1 definition of "law enforcement".
48 *FOIPPA* s. 33(3)(d).
49 *FOIPPA* s. 27(3)(a).

RESOURCES

Privacy Guidelines for Public Libraries webinar series
This free, online series can help library directors and library staff better understand how the ***Freedom of Information and Protection of Privacy Act*** (*FOIPPA*) applies to B.C.'s public libraries. A companion resource to these guidelines. Available through the Northwest Library Federation website, www.nwlf.ca

Laws And Regulations

- ***Freedom of Information and Protection of Privacy Act,*** RSBC 1996, c. 165
  - https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi
- ***FOIPPA* Regulation,** B.C. Reg. 155/2012
  - https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/155_2012
- **Privacy Impact Assessment Directions**, Minister of Citizens' Services Direction 2-21
  - 2021 PIA Directions for NON Ministries - Final (gov.bc.ca)
- ***Library Act*,** RSBC 1996, c. 264
  - https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96264_01

OIPC Materials

- Public Libraries may email privacy questions to the OIPC at info@oipc.bc.ca.
- **OIPC's Privacy Guidance Documents**
  - https://www.oipc.bc.ca/resources/guidance-documents/, including:
    - **Security**: "Securing personal information: A self-assessment for public bodies and organizations", October 30, 2020.
    - **FOI Access Requests**: "Tip Sheet: 10 tips for public bodies managing requests for records", January 17, 2018.

      Employee Management:
      - "Employee Privacy Rights", November 8, 2017
      - "Guide to Using Overt Video Surveillance", October 25, 2017
      - "Checking References: Guidance for Public Bodies", November 10, 2014
    - **Accountability/Transparency: "Accountable Privacy** Management in BC's Public Sector", June 26, 2013.
- **OIPC Orders and Decision**
  - OIPC's Website: https://www.oipc.bc.ca/rulings/orders/
  - CanLii, the Canadian Legal Information Institute's free resource for access to judgements
    - https://www.canlii.org/en/#search/id=bcipc

BC Government Resources

- **Privacy & Personal Information Resources** (including guidelines, tip sheets, templates, forms, and other *FOIPPA*-related information)
  - https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/resources
- Individual support is available through the **Privacy Helpline**: 250 356-1851, Privacy.Helpline@gov.bc.ca
- ***FOIPPA* Policy & Procedures Manual,** a reference tool that provides an overview of *FOIPPA* requirements, specific provisions and application examples
  - https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual
- **Privacy Training – *FOIPPA* Foundation**s, a free, interactive, online course on privacy and access fundamentals in BC for public body employees in the broader public sector, as well as BC government employees and contracted service providers:
  - https://mytrainingbc.ca/*FOIPPA*/
- **Privacy & Personal Information in the Public Sector Information Hub**, including Guide to Good Privacy Practices, Privacy Impact Assessment, Agreements, Contracts & Consents, Privacy Breaches, Training, and Templates and Forms: https://www2.gov.bc.ca/gov/content/governments services-for-government/information-management-technology/privacy

TEMPLATES

Collection Notice Templates[50]

[Optionally: include a **preamble** to describe the program, activity or services, to provide a background or context.]

Your personal information is collected by [(name of Public Library) or (name of service provider on behalf of name of Public Library)] under the authority of BC's ***Freedom of Information and Protection of Privacy Act*** [s. 26 or other section] and the BC *Library Act*, [and if applicable, include any other relevant authority authorizing the collection], for purposes of [describe purposes (i.e. "for purpose of administering your library registration and providing you library services")]. The personal information collected includes [list personal information]. Should you have any questions about the collection

of this personal information please contact [Position Title, business address or email address, business phone number].

Sample Collection Notice #1 – Registration

The information on this form is collected by ABC Public Library under the authority of BC's *Library Act* and BC's *Freedom of Information and Protection of Privacy Act*, s.26. The information will be used to administer your ABC Public 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 Public Library's Privacy Officer at abcprivacy@abclibrary.ca, 555-1234.

Note that this sample Collection Notice does not list the personal information collected, as that is encompassed by the opening phrase "the personal information on this form".

Sample Collection Notice #2 – Service Provider

ABC Public Library collects your personal information through Vroom Video Communications ("Vroom") under the authority of BC's *Library Act* and BC's *Freedom of Information and Protection of Privacy Act*, s.26 for the purpose of attending or participating in online video or audio ABC Public Library programs.

The personal information collected by ABC Public Library includes your display name, which may include your first and last name if you choose to enter them, and other information you upload, provide, or create while attending a Vroom session. Certain programs events may be recorded by ABC Public Library. As a result, ABC Public Library may also collect your image, voice, name, personal views and opinions. You will be informed prior to the beginning of the session whether the session is being recorded.

Vroom may collect information about your device, network, and internet connection (e.g., IP address(es), MAC address, device type, operating system, and client version) and information about your usage of or the interaction with Vroom products. This information is not accessible to ABC Public Library. Vroom is located in the US with data centers deployed globally. Vroom's privacy policy is available here [link].

For questions about the collection or use of your personal information, please contact ABC Public Library's Privacy Officer at abcprivacy@abclibrary.ca, 555-1234.

50 A less-detailed template for collection notices is also available on the BC Government's Collection Notice Guidance page.

Consent for Use and/or Disclosure of Personal Information Template

The following template is based on the consent form template available on the BC Government website.

Section 1: Consent

I, <insert name>, consent to the (check all that apply):

☐ use

☐ disclosure

by <insert name of Public Library>of the following personal information: <describe the personal information>.

☐ I am acting on my own behalf; or

☐ I am acting on behalf of another individual <insert name of other individual here> and I have provided evidence that I have the legal authority to do so.

Section 2: Use (Complete this section if relying on consent for use. Delete section if not applicable)

The personal information will be used for <describe the specifics of how it will be used>.

Section 3: Disclosure (Complete this section if relying on consent for disclosure. Delete section if not applicable)

The personal information will be disclosed for the purpose(s) of_<describe the purpose for the disclosure of personal information>.

The personal information will be disclosed to: <insert name(s) of recipient(s)> in/from the following jurisdiction(s): <specify jurisdiction(s), where practicable, or state "N/A" if not practicable>.

Section 4: Signature

This consent is valid from the date signed until: <insert expiry date, if applicable, or state "N/A" if expiry date is not applicable>.

_____ _____

Date Signature

_____

Parent or Guardian Name and Signature (if consent is for a minor under age 12)

Privacy Impact Assessment Template

See the PIA template for "non-ministry public bodies" available through the BC Government website.

Privacy Protection Schedule Templates

Available through the BC Government website, public libraries and other public bodies are welcome to adapt the templates available for cloud services and non-cloud services to suit their needs.

Public Library Privacy Policy Template — General

This sample website privacy policy was written to help Public Libraries develop their own general privacy policies. Care should be taken to ensure that the policy accurately reflects the personal information practices of the individual Public Library. Each Public Library is responsible for its own compliance with *FOIPPA* and should use its own best judgment in discharging its duties under *FOIPPA*.

ABC Public Library — Privacy Policy

[Last reviewed: Date]

Introduction

ABC Library is committed to protecting personal privacy. Any personal information collected, used or disclosed by ABC Library is in accordance with the *Freedom of Information and Protection of Privacy Act* (*FOIPPA*).

Purposes for Which Personal Information May be Collected

ABC Library only collects personal information as permitted by *FOIPPA*. The primary purposes for which ABC Library collects personal information is for the proper administration of Public Library services and programs and the planning and evaluating of services and programs or purposes consistent with this. Such purposes include, but are not limited to, providing access to library materials, services and programs, room rentals, communications, collection of fines, fees and debts, fundraising, evaluating and improving services, and protection of ABC Library property, security of users and staff.

Patrons who do not wish to be contacted about Public Library services and programs or for fundraising or marketing purposes may choose to opt-out of those communications.

Collection and Use

ABC Library collects and uses personal information in accordance with *FOIPPA* to conduct library business, to provide library services and programs and to evaluate, plan and enhance services and programs.

Personal information will only be collected in accordance with *FOIPPA*. Accordingly, 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. In addition, at the time of collection (or before), individuals are informed of ABC Library's legal authority for collecting the information and the name, title, and contact information for ABC Library's Privacy Officer, responsible for ensuring compliance with *FOIPPA*, to whom questions about the collection can be directed.

Unless an individual consents to some other use, personal information will only be used for the stated purpose for which it is collected. Personal information may be collected for uses such as: access to library materials, services, and programs; room rentals; communications; collection of fines, fees, and debts; fundraising; protection of ABC Library property; security of users and staff; non-identifying statistical purposes; and in the limited circumstances provided for in *FOIPPA*.

ABC Library will take reasonable steps to ensure that the personal information held by it is accurate, complete, and up-to-date. ABC Library will correct an individual's personal information if it learns from the individual that the information is incorrect.

Protection of Personal Information

ABC Library uses reasonable security measures to 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.

ABC Library will not retain any personal information longer than necessary for the provision, evaluation, and planning of library services and programs, unless a longer period is required by law.

Access, Accuracy and Correction

Members of the public have access to their own personal information. Access to recorded personal information about a member of the public is provided to that individual upon verification of identity. To request access to your personal information, submit a written request to ABC Library's Privacy Officer (see contact information below). Your request should provide enough detail to enable a Public Library employee to find the personal information.

ABC Library will endeavour to ensure the personal information is as accurate, complete and up-to-date.

You have a right to request that your personal information held by ABC Library be corrected if you believe it is incorrect. You may do so by submitting your request in writing to the Privacy Officer (see contact information below).

Children/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 his/her personal information, the child's parent or guardian may do so on their behalf.

ABC Library assumes that children 12 years are generally capable of exercising their own rights for policy purposes. However, ABC Library 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.

Disclosure

ABC Library will not rent or sell personal information. ABC Library will not disclose personal information to third parties except in accordance with the exceptions permitted under *FOIPPA* including as set out below or with an individual's consent.

Service Providers to the Library

ABC Library ensures that any service providers requiring access to personal information to deliver services on behalf of ABC Library treat personal information in compliance with *FOIPPA*.

Providing some library products and services may require that ABC Library shares personal information with a service provider and/or that an individual shares personal information to create a separate account with the service provider. ABC Library may disclose personal information to a collection agency or credit bureau for the purpose of collecting a debt.

Vancouver Public Library Foundation and Friends of the Vancouver Public Library

Provided an individual has consented to the disclosure, personal information may be disclosed to the [Foundation name] for fundraising purposes.

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.

Emergency Situations

ABC Library 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.

Retention

How long ABC Library keeps your personal information depends on the purpose for which the information was collected.

If ABC Library uses your personal information to make a decision that affects you, we must keep that information for at least one year so that you have an opportunity to access it.

Otherwise, the Public Library 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.

Changes to this Privacy Policy

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

Privacy Officer Contact

If you have any questions or concerns about this policy or how ABC Library treats your personal information, you may contact ABC Library's Privacy Officer at [insert contact information].

2023

Privacy Guidelines for BC Public Libraries

bit.ly/45E3fCk

BRITISH COLUMBIA