**Privacy Management Program
Implementation Toolkit**

**Summer Conference 2023**



**Privacy Program Implementation Tool Kit
Table of Contents**

|  |  |
| --- | --- |
| **Privacy Management Program**  |  |
| Overview | 1 |
| Principles of Privacy and Organizational Obligations | 2 |
| **Getting Started** |  |
| Appoint a Privacy Officer | 6 |
| Supports and Reporting Mechanisms | 6 |
| Conducting a Personal Information Inventory | 7 |
| Personal Information Inventory Checklist | 8 |
| **Policy and Protocol Development** |  |
| Overview | 9 |
| BCTF Privacy Policy | 10 |
| Retention Flow Chart | 13 |
| Sample Retention Protocol | 14 |
| Sample Privacy Breach Protocol | 15 |
| Sample Complaint Investigation Protocols | 17 |
| Sample Access Request Protocol | 18 |
| Sample Access Request Form | 19 |
| Third Party Transfers | 20 |
| **Securing Personal Information** |  |
| Overview | 21 |
| Safeguard Checklist | 22 |
| Best Practices Checklist | 23 |
| Sample Confidentiality Acknowledgement Form | 24 |
| **Organizational Commitment** |  |
| Summary | 25 |
|  |  |
| **Resources** | 26 |

**Overview
Privacy Management Program**

The *BC Personal Information Protection Act* (PIPA) governs the collection, use and disclosure of personal information by private sector organizations, including unions. Itis designed to protect the personal information of individuals while also recognizing when organizations can reasonably collect, use, and disclose personal information.

The BCTF is covered by PIPA, as are the individual locals within the Federation.

Public organizations, including school districts, are governed by the *Freedom of Information and Protection of Privacy Act* (FIPPA). The Office of the Information and Privacy Commissioner oversees the implementation and enforcement of both and provides resources to support compliance. <https://www.oipc.bc.ca/>

Compliance with PIPA requires adherence to fair information practices, sometimes referred to as “Ten Principles of Privacy Protection”

1. Be accountable
2. Identify the purpose
3. Obtain consent
4. Limit collection
5. Limit use, disclosure and retention
6. Be accurate
7. Use appropriate safeguards
8. Be open
9. Give individuals access
10. Provide recourse

[*https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information/principles*](https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information/principles)

An accountable organization must establish, maintain, review and promote those policies and procedures which together will ensure the protection of all personal information under its control in a manner that is compliant with the act and consistent with the above principles. Viewed as a whole, those policies and procedures constitute the organization’s privacy management program.

**Principles of Privacy and Organizational Obligations**

|  |  |  |  |
| --- | --- | --- | --- |
| **PRINCIPLE** | **OBLIGATIONS** | **ACTIONS** | **CONSIDERATIONS** |
| **BE ACCOUNTABLE** | Responsibility for all personal information under the control of the union. This includes information obtained in any manner and how that information is retained, used, or shared.Compliance with Ten Principals | * Designate a Privacy Officer and communicate the identity of the officer to staff, members and the public.
* Develop policies and practices for handling personal information and any privacy complaints.
* Train staff and officers.
* Provide policies to staff, officers and volunteers who encounter personal information and have them sign a confidentiality acknowledgement.
 | Does this person have:* the knowledge to oversee the program?
* the authority to ensure compliance?
* the necessary supports to develop a program?

How will you transfer knowledge to a new Privacy Officer and/or incoming elected officers?What will your training cycle be? When developing policy or making privacy decisions, consider what a reasonable person would feel is appropriate and expect from the union. |
| **IDENTIFY PURPOSE** **↓****OBTAIN CONSENT** **↓****LIMIT COLLECTION** | Identify and clearly communicate the purposes for which the information is being collected.Obtain consent before or when collecting personal information.Collect only the information that is required for fulfilling the stated purpose. | * Conduct an inventory of personal information held by your local.
* Review, and revise as needed, all forms to ensure that the purpose for collection is clearly identified and that the requested information is necessary to fulfill that purpose.
 | Does its use align with the purpose for which it was collected? Ensure consent is clear. It is best to have consent in writing.General consent signed by members on admission to the union may not be sufficient when dealing with highly personal information. Express consent may be needed to access member’s full personnel file, copies of medical reports, and other types of information that members may not expect the union to have automatic access to. |

|  |  |  |  |
| --- | --- | --- | --- |
| **PRINCIPLE** | **OBLIGATIONS** | **ACTIONS** | **CONSIDERATIONS** |
| **LIMIT USE, DISCLOSURE, AND RETENTION** | Ensure that information is used and disclosed only for authorized purposes and in a manner that a reasonable person would deem appropriate.Ensure that information is not kept for longer than is necessary.Ensure that documents are securely destroyed.  | * Share information on a need-to-know basis only.
* Establish role-based access to information.
* Establish a retention schedule.
* Review email practices.
* Ensure that all documents containing personal information are shredded and that all hard drives are cleaned or destroyed when no longer needed.
 | Where are historical files kept?Can you easily locate, retrieve, and permanently destroy any emails that contain an individual’s personal information? Remember that PIPA requires you to keep personal information for at least one year if the information was used to make a decision that affects the member (s. 35). In many instances, a union will need to keep information about members longer than that in order to properly represent them. REMEMBER: The organization is accountable for the lifecycle of the information. |
| **ENSURE ACCURACY** | Make every reasonable effort that the information kept is accurateCorrect incorrect information when requested by the individual or discovered by the organization. | * Ensure that training in systems and procedures is current, in order to minimize process or documentation errors.
 | Individuals have the right to request access—but an organization does not have to correct the information if it does not agree with the request. It does have to make a note that the correction request was made. |

|  |  |  |  |
| --- | --- | --- | --- |
| **PRINCIPLE** | **OBLIGATIONS** | **ACTIONS** | **CONSIDERATIONS** |
| **ESTABLISH SAFEGUARDS** | Ensure the security of all personal information held by your local, by establishing appropriate administrative, physical and technical safeguards. | * Review necessary safeguards and implement those that are missing.
* Establish practices which promote security and minimize risk.
* Keep sensitive personal information in distinct files organized by member.
* Organize materials chronologically.
* Use caution when taking paper materials out of the office. Minimize, put loose papers in binders or envelopes, use locking briefcases.
 | What safeguards are in place? How do you transfer physical and electronic files from one President / Officer to the next? To out of office meetings?Where are historical files kept?Who has access to personal information? Limit and ensure individuals understand obligation to access only on a need-to-know basis?Are the passwords for generic email addresses (e.g., lp@bctf.ca) protected and changed regularly?When privacy breaches occur review practices and implement strategies to prevent similar breaches. |
| **BE OPEN** | Make known and available the contact information of the Privacy Officer.Make available information on policies and practices, including information on the complaint process. | * Determine how to make accessible the local’s privacy policy.
* Develop privacy breach protocols,
 | Website? Other?Any privacy breaches should be reported to the Privacy Officer. In the event of a breach, review the information that was subject to an authorized disclosure and determine if it should be reported to the individual affected. If the breach has serious consequences, it may be necessary to report to the Privacy Commissioner.If uncertain, contact Legal Services with any queries and for advice. |
| **GIVE INDIVIDUALS ACCESS** | Respond to access requests within 30 business days. Response must include:* Personal information that is being disclosed.
* Legal rationale for any information that is withheld.
* Identification of Privacy Officer for further questions.
* Information about requesting a review from Privacy Commissioner.
 | * Develop access protocols.
* Develop an access request form.
 | Unlike FIPPA, PIPA only requires disclosure of the personal information of the individual making the request. There is no right under PIPA to access information held by the union that is not the requester’s own personal information. All documents must be carefully reviewed before disclosure. Be careful not to inadvertently disclose third party information (e.g. another member’s personal information) or information with is privileged (legal advice) and other confidential communications may be exempt from disclosure).Locals should consider reviewing materials with Field Service and Legal Services prior to disclosure. |
| **PROVIDE RECOURSE** | Investigate all complaints using an established investigation protocol. | * Develop a complaint response protocol.
 | Contact Legal Services for advice in the event of a complaint. |

**Getting Started**

**Appoint a Privacy Officer**

A Privacy Management Program begins, therefore, with the appointment of a Privacy Officer. The Privacy Officer is responsible for implementing and overseeing procedures and practices which ensure compliance with the act.

**Considerations**

Questions to consider in determining the appointment of a Privacy Officer and the reporting mechanism through which the Privacy Officer will communicate to the organization include:

* Will the Privacy Officer have the authority to place expectations on other officers, volunteers and staff with regards to privacy practices?
* Will the Privacy Officer be regularly in the local office? If not, what protocols will be in place to provide them with an access adequate enough to facilitate meaningful oversight?
* What administrative supports will exist as the Privacy Officer develops policies and outlines expected practices?
* What other roles/positions will work with the Privacy Officer and provide assistance and input into the development of those policies and practices?
* How will this person be trained? How will this person train others?
* How will the Privacy Officer report to the organization on the Privacy Management Program?

**Provide Supports for Privacy Officer and Establish a Reporting Mechanism**

Although the Privacy Officer will hold both the responsibility for implementing the plan and the authority for enforcing it, the organization is ultimately responsible for overall compliance:

In order to meet its obligations under the act, the organization must ensure that the Privacy Officer has the necessary supports and authority within the organization to assess compliance, implement policies, and establish and improve procedures.

The BCTF provides materials for its staff and locals to support the work of Privacy Officers.

Equally important, the organization must establish a reporting mechanism that ensures that it is up-to-date on issues and is able to evaluate whether or not the Privacy Management Program is adequate. All access requests and complaints should be communicated to the Privacy Officer.

Locals should carry out an annual review of privacy practices and ensure training for staff and officers.

**Conduct an Inventory of Personal Information**

PIPA’s identified purpose is to govern the collection, use, and disclosure of personal information by organizations. Compliance with the act, therefore, requires full awareness by an organization of the type and amount of information it collects, including the sensitivity of that information and the location where it is held.

Conducting an inventory is an essential initial step in ensuring that the information has been correctly collected, that it is being used in connection with the purpose for which it was collected, that it is protected throughout its lifecycle and that it will be destroyed in accordance with an established retention schedule.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Type of Information** |  | **Why is it collected?** | **How is it used?** | **Who has access to it?** | **With whom is it shared?** | **Stored in email.**  | **Is in electronic****files or databases.** | **Is in physical files.** | **Stored in notebooks or phone logs**  |
| **Medical** | Short Term Disability  |  |  |  |  |  |  |  |  |
|  | Long Term Disability  |  |  |  |  |  |  |  |  |
|  | Health and Wellness Program  |  |  |  |  |  |  |  |  |
|  | Accommodation request info |  |  |  |  |  |  |  |  |
|  | Other medical |  |  |  |  |  |  |  |  |
|  | WCB |  |  |  |  |  |  |  |  |
| **Financial** | Bank account |  |  |  |  |  |  |  |  |
|  | RRSP info |  |  |  |  |  |  |  |  |
|  | Pension info |  |  |  |  |  |  |  |  |
|  | Credit / loan info |  |  |  |  |  |  |  |  |
| **Professional** | Concerns and issues |  |  |  |  |  |  |  |  |
|  | Discipline |  |  |  |  |  |  |  |  |
|  | Performance evaluation |  |  |  |  |  |  |  |  |
|  | Peer support info |  |  |  |  |  |  |  |  |
|  | Internal mediation info |  |  |  |  |  |  |  |  |
|  | Code of Ethics  |  |  |  |  |  |  |  |  |
|  | Teacher Regulation Branch |  |  |  |  |  |  |  |  |
|  | Education info |  |  |  |  |  |  |  |  |
|  | Work history |  |  |  |  |  |  |  |  |
|  | Personal references |  |  |  |  |  |  |  |  |
|  | School assignment |  |  |  |  |  |  |  |  |
|  | Benefit information |  |  |  |  |  |  |  |  |
| **Legal** | Criminal allegations |  |  |  |  |  |  |  |  |
|  | Legal Aid  |  |  |  |  |  |  |  |  |
| **Member Info** | SIN |  |  |  |  |  |  |  |  |
|  | Birthday |  |  |  |  |  |  |  |  |
|  | Gender |  |  |  |  |  |  |  |  |
|  | Home Address |  |  |  |  |  |  |  |  |
|  | Phone Number |  |  |  |  |  |  |  |  |
|  | Email address |  |  |  |  |  |  |  |  |
|  | Emergency contacts |  |  |  |  |  |  |  |  |
|  | Family  |  |  |  |  |  |  |  |  |

**Policy and Protocol Development: Overview**

PIPA requires that all organizations create policy and practices that ensure compliance with the act.

PIPA Part 2, Section 5—Policies and Practices ([link](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01#section5))

1. *Develop and follow policies and practices that are necessary for the organization to meet the obligations of the organizations under this Act*
2. *Develop a process to respond to complaints that may arise respecting the application of the Act, and*
3. *Make information available on request about*
4. *The policies and practices referred to in paragraph (a), and*
5. *the complaint process referred to in paragraph (b)*

It is recommended that all locals create the following:

* Privacy Policy
* Retention Policy
* Privacy Breach Protocols
* Complaint Processing Protocols
* Access Request Protocol
* Best Practices Instructions.

BCTF Privacy Policy

The British Columbia Teachers’ Federation (BCTF) is committed to protecting the privacy and confidentiality of its members’ personal information.

The BCTF is committed to complying with the British Columbia *Personal Information Protection Act*, S.B.C. 2003, c. 63 (PIPA). This includes managing the collection, use, disclosure, retention, and ultimate disposition of its members’ personal information in ways that safeguard the privacy of its members.

**Definitions**

*Personal Information*—means information about identifiable individuals and includes employee personal information but does not include contact information, or work product information.

*Privacy Officer*―means the staff person designated responsibility for ensuring that the BCTF complies with this policy and PIPA.

**Personal information collected**

The BCTF collects personal information to fulfill its obligations to members and in the course of providing a variety of services. The types of information collected include:

* name
* home address and telephone number
* birth date
* home email address.

Additional information may be collected to administer the collective agreement, to fulfill the BCTF’s duty of representation to you, or to provide you with specific services.

**Purposes for collection, use, and disclosure**

The BCTF collects, uses, and discloses personal information for the purposes of fulfilling our obligations to you as set out in the BCTF *Members’ Guide*, to provide specific services as required, and to fulfill its role as the bargaining agent representing members. The purposes for which the BCTF collects, uses, and discloses personal information include, for example:

* to identify you
* to communicate with you
* to confirm your eligibility for services
* to comply with various professional legal and regulatory requirements
* to provide services related to the Salary Indemnity Plan, legal services, grievances, Workers’ Compensation Board (WorkSafe BC) advocacy, Ministry of Education Professional Conduct Unit (formerly Teacher Regulation Branch) advocacy, and pension plan advocacy and assistance
* to provide provincial specialist association memberships and associated services
* to conduct research.

**Protection of personal information**

The BCTF is committed to protecting your personal information from unauthorized use or disclosure. Its commitment means that:

* it will use your personal information only for the purposes it has identified.
* it will not disclose your personal information without your permission unless it is required or authorized by law to do so.
* it will employ appropriate security measures to ensure only authorized individuals have access to your personal information.
* it will keep your personal information only as long as is reasonably necessary.
* it will destroy your information using a confidential and secure method when your personal information is no longer required.

**Individual access**

Individuals have the right to request access to their personal information under the control of the BCTF. The Privacy Officer will assist them with their access requests.

Access requests must be submitted by completing the BCTF Access Request Form. You may request a form by sending an email to the BCTF Privacy Officer and returning the form by mail to the BCTF, 100 – 550 West 6th Avenue, Vancouver, BC, V5Z 4P2, Attention Privacy Officer; alternatively, the form can be submitted to the BCTF Privacy Officer electronically by sending it as an attachment in an email to *privacy@bctf.ca*. In certain situations, further to privacy legislation, the BCTF may not be able to provide access to certain personal information that it holds about an individual. Examples of where it may not provide access include, but are not limited to, situations where:

* the provision may reveal personal information about another individual.
* the information is subject to solicitor-client privilege.
* the information was collected in relation to an investigation or a contravention of a federal or provincial law.
* the provision could reasonably be expected to threaten the health or safety of an individual.

If access cannot be provided, the BCTF will notify the individual making the request, in writing, of the reasons for the refusal. Where access has been provided and where the information is demonstrated to be inaccurate or incomplete, the BCTF will amend the information as required. Where the information needs to be provided in an alternative manner to ensure the health of safety of the individual, the BCTF will notify the individual making the request.

**Questions or concerns regarding BCTF’s privacy procedures**

An individual may direct their general questions regarding privacy at the BCTF, as well as any questions or concerns regarding BCTF’s compliance with this policy, by mail to the BCTF at 100 – 550 West 6th Avenue, Vancouver, BC, V5Z 4P2, Attention Privacy Officer or by email to *privacy@bctf.ca*.

The BCTF will investigate any complaints received in writing. If a complaint is found to be justified, the BCTF will take appropriate measures to resolve the complaint including, if necessary, amending its policies and procedures. An individual will be informed in writing of the outcome of the investigation regarding their complaint.

**Developing a Personal Information Retention Policy**

Does the record contain personal information?

Yes

No

Is there a “business reason” to keep the information?

Yes

No

Who is responsible for the file? Who has carriage (e.g. grievance)?

BCTF

Local

Does the BCTF have a retention policy for this type of information?

Yes

No further action required.

No

Destroy the information in a secure manner after one year.

Check that BCTF has necessary information and destroy in a secure manner.

Ask BCTF (via FSD); check legal statutes.

If unable to determine a retention period, keep the information for as little time as necessary.

Use new retention period.

Use same retention period, if possible.

**Sample Personal Information Retention Periods**

|  |  |  |
| --- | --- | --- |
| **File Type** | **Retention Period** | **Notes** |
| Member files, general | Minimum of 1 year then cull regularly | Keep only as long as needed |
| Grievance, non-precedential resolution | 10 | Keep longer than 10 years only if there is a purpose for doing so |
| Grievance-precedential | 10 years for background documents and materials | Precedential materials—keep record of grievance letter and grievance resolve permanently.Background documents containing personal information should be removed from file and securely destroyed. |
| Grievance referred to arbitration | 20 years for background documents and materials | Precedential materials—keep record of grievance letter and grievance resolve permanently. |
| Grievance resolved through arbitration hearing | 20 years for background documents and materials | Arbitration decision—keep permanently. |
| Grievance, physical contact with students | 35 years |  |
| Legal records | 20 years |  |
| Code of ethics | 10 |  |
| Peer support | 10 |  |
| Health and Safety | 10 |  |
| Privacy—Access Requests | 1 |  |
| Medical Records | 1 | Medical records not associated with a case file (i.e. grievance, LTD, etc.) should not be kept for an extended period. |
| Rehabilitation, Return to Work | 10 |  |
| Resumes, CVs, applications | 1 year |  |

Note: retention periods begin when file is closed, not the date of individual documents.

**Sample Privacy Breach Protocol**

|  |  |  |
| --- | --- | --- |
| **STEPS** | **QUESTIONS** | **ACTIONS and CONSIDERATIONS** |
| 1. **CONTAIN THE BREACH**
 | Is the breach the result of a systemic issue? | e.g., incorrectly recorded contact information —immediately correct this. |
| Retrieve the information | Is an unauthorized person/organization in possession of the breached information? | Make every effort to retrieve the information from the person/organization; inform the person/organization of their obligation under PIPA to ensure that no unauthorized copy of the information has been stored or shared.  |
| Review the breach | How did it happen? |  |
|  | Why did it happen? | e.g., Human error, lack of training, system malfunction. |
|  | When did it happen? |  |
| Review security | What security features were in place? |  |
|  | Which worked and which didn’t? | Determine if new practices or security measures are needed. |
| 1. **EVALUATE THE RISKS**
 | Whose information was compromised? |  |
|  | What kind of information was compromised? | Financial, medical, marital, professional, disciplinary, etc.Is it of low or high sensitivity? |
|  | Were any identifying numbers compromised? | SIN, Member ID, driver’s licence, health care number, credit card number, bank account, etc. |
|  | What type of harm could result? | Identity fraud? Harm to reputation?  |
| 1. **NOTIFICATION**
 | Affected individuals* determine if notification is appropriate
* if so, speak to individuals by phone and send a follow up email or letter
 | Privacy Officer must analyse the breach to determine if there is a risk of harm. Local Privacy Officers may need to reach out to BCTF Field Service and Legal Services.Where there is a risk of significant harm, it may be necessary to notify the Privacy Commissioner and in some cases the police.Even where the risk of harm is low, generally, the affected individual(s) will need to be notified. The content of the notification should include:* date of the breach (if known)
* date breach came to organization’s attention
* description of the personal information that was disclosed
* description of any potential harms
* description of steps taken to contain breach and reduce harm
* steps the individual can take (how to contact credit reporting agencies etc.)
 |
|  |  | * contact information for follow up questions or further info
* description of any other steps the organization has taken to address the breach including any report to the police or Privacy Commissioner (for very serious breaches), internal review, changes to future practices
 |
|  |  |  |
|  | The Privacy Commissioner  | If there is a significant risk of harm, the organizations should consider: |
|  | Should the police be contacted? | Providing members with the names and contact information of issuing organizations of breached information (e.g., Motor Vehicle Branch if driver’s licence lost).Paying for Equifax for credit reporting and monitoring if there is a risk of identity theft and/or financial information is compromised.If no risk of significant harm, analyze the breach in terms of member confidence, local reputation, and transparency. |
| 1. **PREVENTION**
 |  |  |
| Review cause of breach |  | Review what led to the breach.  |
| Document the breach |  | Keep records of all privacy breaches. Organize in chronological files. |
| Review practices and procedures |  | Consider whether any changes are needed to policies and practices to prevent similar breaches. |
| Training |  | Schedule a time for an annual review of the privacy management program. Staff and officers who handle personal information should be trained at regular intervals through BCTF training and or using training materials available from the Privacy Commissioner: <https://www.oipc.bc.ca/guidance-documents/1428> <https://www.oipc.bc.ca/privacyright/webinars/webinar-8/>  |

**Sample Complaint Investigation Protocol**

|  |  |
| --- | --- |
| **ACTION** | **CONSIDERATIONS** |
| Open a file | Maintain a file numbering system of complaints received. |
| Record the date of the complaint |  |
| Record the nature of the complaint | e.g., delay in response time; improper use or disclosure, inaccuracy of information.  |
| Send an acknowledgment letter to the complainant | Inform the complainant that the complaint is being investigated and give an approximate time frame for the investigation. |
| Assign the investigation to a skilled impartial person  | Ensure that this individual is given access to all relevant records and files and the authority to interview relevant individuals. |
| Notify individuals of outcome of the investigation | Outline any steps taken in the investigation, the outcome and any actions that will flow from it, i.e., training, review of systems etc.—NOT disciplinary records or sanctions.  |
| Correct any inaccurate information |  |
| Review and improve procedures, security and or training as per the outcome |  |

**Sample Access Protocol**

|  |  |  |
| --- | --- | --- |
| **STAGES** | **ACTIONS** | **CONSIDERATIONS** |
| Administrative preparations | * Establish a fee schedule.
 | Fees should be minimal and reasonable. |
|  | * Implement a file naming system for requests and locate a secure filing area for these requests.
 |  |
| Communicating the process | * Privacy Policy informs individuals how to request access to their information.
 |  |
|  | * Access request form is readily accessible to individuals.
 |  |
|  | * Access form clearly outlines the fee schedule.
 |  |
| Processing the request | * Date stamp the access form.
* Calculate the 30 business day timeline.
 | PIPA requires a response within 30 business days. |
|  | * Do an initial assessment of request to see if it is possible to complete the request within the required timeline.
* If not, send a letter indicating that a delay may be necessary, indicate the expected response date and inform them of their right to complain to the Commissioner.
* See PIPA Section 31.
 | All efforts should be made to respond within 30 business days.NOTE: This will be a very rare occurrence but could happen if the scope of the request is so large and/or so complicated that 30 business days might not suffice. |
| Accessing the request | * Assemble all the requested information.
* Review the information against Section 23 of PIPA.
* Seek legal advice if there are grey areas
 | Depending on the request, review physical files, emails, notes, and electronic files for requested info. Seek legal advice if PIPA might prohibit release. |
| Withholding or redacting information | * Send letter to applicant explaining the reasons for the withholding of information and inform the applicant of the right to appeal to the Commissioner.
 |  |
| Releasing the information | * Notify applicant of costs to confirm if the applicant still wants to proceed.
 | This is necessary if the costs are significant.  |
|  | * Assemble the information to be released.
 |  |
|  | * Make a copy of released information.
 |  |
|  | * Send letter (include date & text of request and date of receipt of request) and requested information to individual in a secure manner.

  |  |

Personal Information Access Request Form - MEMBERS

Date of Request:

## Request for Information

To process your request, we require the following information:

Full Name (Please print):

Address:

Relationship to Local (i.e. member, retired member):

Membership Number (if applicable):

Contact Phone #(s):

The [Local] stores information in a number of databases and files. To enable us to process your request quickly and efficiently, please outline as specifically as possible the information you would like to receive and any committees, grievances or files with which it may be associated. We will begin processing your request as soon as this form is completed and received by the Local’s Privacy Officer. We will make all attempts to respond within 30 business days of receipt of your request.

|  |
| --- |
| Information requested: |
| This information is associated with the following:1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 |

Requestor Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This form should be placed in an envelope marked “Confidential” and mailed to: Privacy Officer, [Local], address. alternatively, the form can be submitted to the Privacy Officer electronically by sending it as an attachment in an email to email address.

**Third Party Transfers**

The protection of personal information, which has been transferred by a Local to third party processors or service providers, remains the responsibility of the Local and the Local must therefore ensure that such information is protected to a similar level that the Local would provide. This could arise where locals use accounting and other professional services.

Locals should only transfer member information to third parties in circumstances where it can be reasonably expected that:

* The third party will respect privacy and confidentiality
* Appropriate safeguards will be in place to maintain the security of the information
* Use and disclosure of the information will be limited to the purposes needed to fulfill the contract
* Any personal information will be returned or securely disposed of upon completion of the contract

.

**Securing Personal Information**

PIPA requires organizations to “*protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks”.*

In reviewing and establishing appropriate safeguards it is important to consider physical, administrative, and technical measures.

* Physical measures should ensure the secure storage of files, the secure access of the building, and the secure destruction of files and hard drives.
* Administrative measures include role-based access to personal information, regular training of Local officers, volunteers and staff, and confidentiality acknowledgements for the same.
* Technical measures include strong password enforcement, encryption where applicable, network safeguards such as firewalls and the wiping clean of all devices before they are discarded, donated, or sold.

The above measures alone are not sufficient but must also be accompanied by practices which promote security and minimize risk. In establishing these office practices, the local should consider how staff, officers, and volunteers:

* maintain the security of filing cabinets, office equipment, and office exteriors
* manage paper flow
* send and receive emails and faxes
* secure laptops and other mobile devices
* access networks and the internet
* use and access software

Lastly, the sensitivity of the information being protected must be considered when determining which safeguards and practices to implement.

Once security measures are implemented and best practices are established it is important to regularly review them to ensure that they remain adequate and adhered to.

**NOTE:** Locals which have home offices should conduct an annual risk audit to ensure that the appropriate physical safeguards are in place.

**Safeguards Checklist**

|  |  |  |
| --- | --- | --- |
| **MEASURES** | **ISSUES** | **ACTION NEEDED** |
| Physical Measures | Entry to office is secure. |  |
|  | File cabinets have locks. |  |
|  | Access to files within office / building is restricted. |  |
|  | The office is equipped with a crosshatch or microcut shredder.  |  |
|  | Computer monitors are positioned so that they are not visible to visitors. |  |
|  | Computer hard drives are destroyed before being discarded. |  |
|  | External hard drives are secured. |  |
| Administrative Measures | Local officers, volunteers, and staff are trained and understand the local’s obligations under PIPA. |  |
|  | Local officers, volunteers, and staff sign confidentiality acknowledgments. |  |
|  | Access to personal information is provided on a role-based model and on a “need-to-know” basis. |  |
| Technical Measures | Access to systems containing personal information is role-based. |  |
|  | Network access and computer access is password protected; passwords are strong and regularly changed. |  |
|  | Networks and computers are secured, where possible, through methods such as firewalls, anti-virus protection, and encryption.  |  |
|  | Hard drives on computers, photocopiers, fax machines are wiped clean or physically destroyed prior to being discarded. |  |

**Best Practices Checklist**

|  |  |  |
| --- | --- | --- |
| **MEASURES** | **PRACTICE** | **ACTION NEEDED** |
| Physical Security | A record of key allocations is kept. |  |
|  | A system is in place for ensuring keys are returned. |  |
|  | Documents are shredded prior to being recycled. |  |
|  | Staff adopt a “clean desk policy” as part of end of day procedures. |  |
|  | Laptops and other mobile devices are not left unattended at any time. |  |
| Fax | Personal information is rarely sent by fax; when it is, phone calls are made prior to sending it to ensure that someone is available to receive it.  |  |
|  | Faxed materials include a cover sheet with a disclaimer about the confidential nature of the information. |  |
| Email | Personal information is transmitted by email ONLY if the individual has agreed to such transmission.  |  |
|  | Personal information is only transmitted on secure *bctf.ca* addresses and never on commercial email.  |  |
|  | Passwords for generic *bctf.ca* addresses are changed when they are reassigned. |  |
|  | Email passwords are never shared. |  |
| Technical Protocols | Users program computer screensavers to function after a short interval of inactivity. |  |
|  | Laptop users turn off file share when accessing public networks. |  |
|  | File sharing sites such as Dropbox and Google Docs are not used for sensitive, personal information transmission. |  |
|  | Unauthorized software is not downloaded onto Local computers. |  |
|  | Access to systems containing personal information is terminated or modified as roles change.  |  |
|  | End of day procedures include instructions for logging off the computer and network. |  |

SAMPLE ACKNOWLEDGMENT FORM

# General Privacy and Confidentiality Acknowledgement

In accordance with British Columbia *Personal Information Protection Act* (PIPA) and applicable local policy, I am aware of the need to protect all personal information to which I have access in the course of my employment / volunteer / elected activities with the local. I understand that I am to use the personal information only for the purposes for which it was collected and purposes consistent with my employment / volunteer / elected responsibilities. I understand that I am to only disclose personal information as required or authorized by law. I understand that discipline or sanctions, up to and including dismissal (as per relative collective agreements), may result if I, through intent or negligence, access, collect, use, disclose, or dispose of personal information without authority. I understand that my legal obligation does not end with my employment / volunteer / elected activities at the local but continues in perpetuity and that failure to keep confidential the personal information of individuals is grounds for legal action.

By my signature I acknowledge that I have read and understand this obligation.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name (Please print) Role

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date

**Organizational Commitment**

Essential components of a successful Privacy Management Program include, therefore, the ongoing assessment, modification, and revisions of privacy policies, practices, training and communications. This review cycle is the final implementation step in establishing a Privacy Management Program which ensures full compliance with all aspects of the act.

In summary, an organization with a robust Privacy Management Program is characterized as one which supports and promotes:

* a strong ethic of privacy.
* an engaged commitment on the part of senior leaders.
* a knowledgeable and involved Privacy Officer who has the authority, resources, and supports to manage the program.
* clear reporting mechanisms for communicating the successes and challenges of the Privacy Management Program and for reporting on security lapses and/or privacy breaches.
* an awareness of the personal information it collects, the purposes for which it collects it, the use the information is put to, the manner in which the information is stored and destroyed.
* the policies and procedures which promote compliance and minimize risk.
* knowledgeable and trained staff, officers, and volunteers.
* openness in communicating with individuals whose personal information it possesses and informing them of their privacy rights.
* a commitment to ongoing training and auditing of policies and practices.

**Privacy Program Resources**

**Office of the Information and Privacy Commissioner for British Columbia**
[*www.oipc.bc.ca*](http://www.oipc.bc.ca)

* A Guide to B.C.’s Personal Information Protection Act for Businesses and Organizations <https://www.oipc.bc.ca/guidance-documents/1438>
* Webinars, videos and podcasts: <https://www.oipc.bc.ca/privacyright/>
* Securing Personal Information: A Self-Assessment Tool for Organizations <https://www.oipc.bc.ca/guidance-documents/1439>
* Privacy Breaches: Tools and Resources <https://www.oipc.bc.ca/guidance-documents/1428>
* Orders, Decisions, Judicial Reviews, Adjudications <https://www.oipc.bc.ca/rulings/orders/>
* Investigation Reports, Special Reports, Mediation Summaries <https://www.oipc.bc.ca/reports/investigation-and-audit-reports/>

 **Government of British Columbia**Protecting Personal Information
[*https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information*](https://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information)

**Legislation**
Personal Information Protection Act—BC
[*https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00\_03063\_01*](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01)