DIGITAL INNOVATION GROUP

Privacy Policy Development

November 10 2020

Table of Contents

Purpose 1

Background 1

Process 1

- Step 1: Assign a privacy officer 2
- Step 2a: Conduct an audit 2
- Step 2b: Conduct a self assessment 2
- Step 3: Develop a privacy policy 3
- Step 4: Implement and maintain the privacy policy 4
- Appendix A 6
  - Audit Questions 6
- Appendix B 9
  - Self Assessment Questions 9
- Appendix C 13
  - Personal Information Protection Policy Template 13

Purpose

The purpose of this document is to provide a common basis for the development of a privacy policy for each of the Digital Innovation Group (DIG) partners.

Background

To collect, use or disclose personal information, private sector organizations in B.C. must follow the personal information and privacy rules set out in the *Personal Information Protection Act* (PIPA).

Personal information includes:

- Name, sex, age, weight, height
- Home address and phone number
- Race, ethnic origin, sexual orientation
- Medical information
- Income, purchases and spending habits
- Blood type, DNA code, fingerprints
- Marital or family status
- Religion
- Education
- Employment information

Of the six Arts Councils that comprise DIG—the Arts Council of Ladysmith and District (ACLD), the Cowichan Valley Arts Council (CVAC), Salt Spring Arts Council (SSAC), Comox Valley Arts (CVA), Hornby Island Arts Council (HIAC), and The Old School House Art Centre (TOSH)—only three entities currently mention privacy policies or practices on their websites—CVAC, SSAC, and TOSH.

Process

In order to develop a privacy policy that complies with PIPA, the provincial government recommends a four step process:

1. Assign one or more individuals as privacy officers
2. Conduct an audit and self-assessment
3. Develop a privacy policy for your organization
4. Implement and maintain your privacy policy

Step 1: Assign a privacy officer

By law, all organizations must assign at least one privacy officer. The title and contact information of each privacy officer must be made available to the public as well as members within the organization.

A privacy officer must be familiar with PIPA and is responsible for:

- Conducting a privacy audit and self-assessment
- Developing a privacy policy
- Implementing and maintaining a privacy policy
- Managing privacy training
- Responding to requests for access to and correction of personal information
- Working with the Information and Privacy Commissioner in the event of an investigation

While DIG has contracted Shannon Delaney to conduct privacy audits and assessments as well as to develop privacy policies for each DIG partner, it is recommended that each organization appoint their own privacy officers to maintain their organization's policy, respond to requests, and comply with investigations.

Step 2a: Conduct an audit

The privacy audit involves taking an inventory of an organization's personal information holdings, and then identifying information needs and practices of the different areas of the organization. See Appendix A for audit questions.

Step 2b: Conduct a self assessment

PIPA is based on the following 10 principles of privacy protection, which an organization must use to assess the results of their own privacy audit:

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

Self assessment questions are required for each of the 10 principles, and a negative response to any question identifies an area in need of improvement. See Appendix B for self assessment questions.

Step 3: Develop a privacy policy

The results of the privacy audit and self-assessment assist with determining the required scope of an organization's privacy policy.

The "Personal Information Protection Policy Template," attached here as Appendix C, can be adjusted to fit a particular organization by completing the highlighted areas.

A privacy policy describes and directs how an organization collects, uses, discloses, stores and destroys personal information in order to comply with the ten principles of privacy protection and PIPA. It must also include a privacy complaint process, which addresses the following:

Who will receive and handle complaints

The organization's privacy officer, who ensures privacy compliance, is also responsible for receiving and responding to internal and external complaints.

How complaints will be handled

For all complaints, the organization will investigate, acknowledge receipt promptly, contact the individual for any required clarifications, follow a fair and confidential process.

How complaints will be accepted

Complaints may be received in writing or verbally, as appropriate for the organization. Whatever method is chosen, it must be articulated clearly, and the procedure must be adaptable, where appropriate, to ensure accessibility.

How customers will be informed about the process

An organization's representatives must be able to explain the privacy complaint process, identify who customers can contact to file a complaint, and inform customers of their right to contact the Information and Privacy Commissioner if unsatisfied with an organization's response.

How complaints will be documented

All privacy complaints must be documented and include the date of receipt.

How process impartiality will be ensured

The person assigned to investigate a complaint must be able to investigate fairly and impartially. Investigation should not be done by a person who is the subject of the complaint. The investigator must have access to all relevant records, employees or other individuals who handled the personal information involved.

How issues identified in the complaint will be corrected

An organization must work to rectify the situation, including correcting practices and policies where necessary and communicating those changes to employees. Every decision made as the result of an investigation must be documented. The complainant must be notified of the outcome and the corrections and preventative steps taken.

Step 4: Implement and maintain the privacy policy

After developing a privacy policy, an organization may need to implement changes to personal information practices and systems related to technology, communications, service contracts, and training.

Changes to Technology

Adopting the compliance standards addressed in an organization’s privacy policy may require changes to information technology systems such as updating databases to make personal information retrievable for individuals upon request or eliminating automatic collection of personal information on a website.

Communications Materials & Forms

Public information may need to be reviewed and revised to comply with the organization’s privacy policy in order to inform customers about updated personal information practices. This may include websites, brochures and promotional material.

Paper and digital forms used to collect personal information should also be reviewed and revised to add information collection notices and clarify the purpose for collecting personal information.

Service Contracts

Organizations are responsible for the personal information they collect, store or control. This includes personal information transferred to a contractor and information a contractor may collect on the organization's behalf.

Service contracts must clearly state the privacy requirements that must be met to comply with an organization’s privacy policy.

Internal Training

All employees, associates, contractors, partners or agents who collect, use or disclose personal information must undergo some form of privacy training. Training programs should outline privacy requirements, expectations and procedures, including:

- The legislative requirements of personal information and privacy (PIPA)
- The ten principles of privacy protection
- The organization’s privacy policy
- Privacy considerations related to specific roles, tasks and responsibilities within the organization

Appendix A

Audit Questions

1. Which departments within your organization collect, access, use or disclose personal information. Departments may include:
    - Customer service
    - Human resources
    - Finance/purchasing
    - Information technology

2. List all of the points of contact within your organization involving personal information, such as:
    - Customer service telephone numbers
    - Points-of-purchase
    - Kiosks
    - Contests
    - E-mails
    - Surveys
    - Video cameras
    - Audio tapes
    - Marketing lists
    - Loyalty programs
    - Delivery services
    - Returns
    - Application forms
    - Order forms
    - Websites
    - Bulletin boards

3. How is the collected information managed and stored? Consider records stored in hardcopy, on internal computers, in other electronic media and in online resources (cloud).

4. Who has access to the personal information held by the organization and who actually needs to have that access?

5. Why does the organization collect the personal information? Is the personal information being collected, used or disclosed actually necessary to a particular function or operation?

6. Are individuals made aware that the organization is collecting their personal information?

7. Does the organization inform individuals of the purpose for collecting their personal information?

8. Does the organization obtain consent from individuals before collecting or using their personal information? If so, what processes are used to obtain consent? (verbal statements, paper or electronic notices etc.)

9. How does the organization use personal information? (for specific business functions, for activities that solicit new business etc.)

10. Does the organization disclose personal information to anyone outside the organization?

11. If personal information is disclosed outside the organization, are individuals aware of the intended uses and disclosures of their personal information? If so, how are individuals informed?

12. Is the personal information the organization holds accurate, complete and up-to-date?

13. Does the organization have measures to protect the personal information it holds from unauthorized access, collection, use, disclosure, copying or modification from individuals both within and outside the organization?

14. Does the organization contract out any functions or activities involving personal information? Does the organization take any privacy measures to protect this information?

15. How long does the organization retain personal information?

16. How does the organization destroy or dispose of personal information?

Appendix B

Self Assessment Questions

These questions can be answered with a simple yes or no. A *no* will indicate an area in need of improvement.

Accountability

1. Has your organization assigned a privacy officer?
2. Has your organization developed and implemented policies and practices for the proper handling of personal information?
3. Does your organization use contracts or other means to ensure that any contractors providing services on your behalf provide privacy protection equal or superior to your own?
4. Has your organization developed and implemented a complaint process to handle complaints about personal information practices?

Purpose

1. Does your organization identify why personal information is needed and how it will be used, taking into account primary and secondary purposes?
2. Does your organization inform individuals, either verbally or in writing, of the purposes for collecting their personal information before or at the time when information is collected?
3. Before using personal information for a new purpose, does your organization inform individuals of the new purpose and obtain consent prior to its use?

Consent

1. Does your organization obtain consent from individuals whose personal information is collected, used or disclosed?
2. When obtaining consent, does your organization inform individuals of the purposes for the collection, use or disclosure of their personal information in a manner that is clear and can be reasonably understood?
3. Does your organization obtain individual consent before or at the time of collection, as well as when a new use is identified?
4. Does your organization obtain consent without using deceptive means or false or misleading information about how the personal information will be used?
5. Does your organization ensure that consent is not a condition for supplying a product or a service unless the collection, use or disclosure of the personal information is necessary to provide the product or service?

6. When determining what form of consent to use (e.g. written, verbal, implied, opt-in or opt-out), does your organization consider both the sensitivity of the personal information and what a reasonable person would expect and consider appropriate?
7. Does your organization permit individuals to withdraw consent to the collection, use or disclosure of their personal information (unless withdrawing consent would conflict with a legal obligation)?
8. After receiving a notice to withdraw consent, does your organization explain the likely consequences of withdrawing consent?

Collection

1. Does your organization collect personal information for a purpose that a reasonable person would deem appropriate?
2. Does your organization limit the amount and type of personal information collected to what is necessary to fulfill the purpose identified before or when it was collected?
3. Does your organization collect personal information directly from the individual unless authorized to collect personal information from another source?

Use, Disclosure, and Retention

1. Does your organization use or disclose personal information for purposes that a reasonable person would deem appropriate?
2. Does your organization keep personal information for only as long as necessary to fulfill the purpose identified before or when it was collected?
3. Does your organization keep personal information that is used to make a decision about an individual for at least one year after using it so the individual has a reasonable opportunity to access it?
4. Does your organization destroy, erase or make anonymous any personal information as soon as it is no longer required for a legal or business purpose?

Accuracy

1. Does your organization make reasonable efforts to ensure that the personal information you collect is accurate and complete?
2. Does your organization minimize the possibility of using incorrect or incomplete information when making a decision that affects an individual or when disclosing an individual's information to another organization?

Safeguards

1. Does your organization make reasonable security arrangements to protect personal information under your control, including physical measures, technical tools and organizational controls where appropriate?
2. Does your organization safeguard personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal by individuals from within and outside your organization?
3. Does your organization protect all personal information regardless of its format, including paper, electronic, audio, and video data?

Openness

1. Does your organization make the following information readily available to customers and employees upon request?
    - The title and contact information of your privacy officer—in order to explain personal information policies and practices or answer questions about the purpose for collecting personal information?
    - The process an individual can follow to gain access to his or her personal information and the title and contact information of the employee an individual can contact to make such a request?
    - Information that explains your organization's personal information policies and practices?
    - The process for making a complaint about your organization's personal information practices?

Access

1. If all or part of an access request is allowed, does your organization provide the individual with:
    - Access to their personal information in the form of a copy of the information requested, within 30 business days (unless an extension of time is permitted in the legislation)?
    - An explanation of how their personal information is or has been used?
    - A list of any individuals or organizations to whom their personal information has been disclosed?
2. If all or part of an access request is refused, does your organization provide the applicant with:
    - A response that includes the legal reason(s) for the refusal, within 30 business days?
    - The title and contact information of your privacy officer if the applicant has questions about the refusal?

- Information on how to request a review by the Information and Privacy Commissioner?

3. For access requests to correct personal information, does your organization:
    - Correct any personal information discovered to be inaccurate or incomplete?
    - If a correction is made, does your organization send a copy of the corrected personal information to each organization for which the incorrect or incomplete information was disclosed in the past year?
    - If no correction is made, does your organization annotate the personal information to indicate that a correction was requested but not made?

Recourse

1. Has your organization developed and implemented simple and accessible complaint handling procedures?
2. Does your organization Investigate all complaints received?
3. Does your organization take appropriate measures to correct information handling practices and policies?
4. Does your organization inform complainants of their avenues of recourse, including your organization's own complaint process and the Information and Privacy Commissioner’s complaint process?

Appendix C

Personal Information Protection Policy Template

This form has been designed to meet the needs of a diverse range of organizations. To make the form reflect the operations of your particular organizations, fill in the appropriate information in all areas highlighted in yellow.

Name of organization

Personal Information Protection Policy

At Name of organization, we are committed to providing our clients, customers, members with exceptional service. As providing this service involves the collection, use and disclosure of some personal information about our clients, customers, members, protecting their personal information is one of our highest priorities.

While we have always respected our clients, customers, members privacy and safeguarded their personal information, we have strengthened our commitment to protecting personal information as a result of British Columbia's *Personal Information Protection Act* (PIPA). PIPA, which came into effect on January 1, 2004, sets out the ground rules for how B.C. businesses and not-for-profit organizations may collect, use and disclose personal information.

We will inform our clients, customers, members of why and how we collect, use and disclose their personal information, obtain their consent where required, and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

This Personal Information Protection Policy, in compliance with PIPA, outlines the principles and practices we will follow in protecting clients', customers', members' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our clients', customers', members' personal information and allowing our clients, customers, members to request access to, and correction of, their personal information.

Scope of this Policy [OPTIONAL SECTION: The Scope section should only be included if applicable]

This Personal Information Protection Policy applies to Name of organization and its subsidiaries, Names of subsidiaries.
This policy also applies to any service providers collecting, using or disclosing personal information on behalf of Name of organization.

Definitions

Personal Information –means information about an identifiable *individual [**OPTIONAL ADDITION**: consider providing examples of personal information your organization collects. E.g., including name, age, home address and phone number, social insurance number, marital status, religion, income, credit history, medical information, education, employment information].* Personal information does not include contact information (described below).

Contact information – means information that would enable an individual to be contacted at a place of business and includes name, position name or title, business telephone number, business address, business email or business fax number. Contact information is not covered by this policy or PIPA.

Privacy Officer – means the individual designated responsibility for ensuring that Name of organization complies with this policy and PIPA.

Policy 1 – Collecting Personal Information

1.1 Unless the purposes for collecting personal information are obvious and the client, customer, member voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

1.2 We will only collect client, customer, member information that is necessary to fulfill the following purposes:

[Fill in the purposes for which your organization collects personal information. Examples of purpose statements, which may or may not be applicable to your organization, include:

- To verify identity;
- To verify creditworthiness;

- To identify [client, customer, member] preferences;
- To understand the [financial, banking, insurance] needs of our [clients, customers, members];
- To open and manage an account;
- To deliver requested products and services
- To guarantee a travel or hotel reservation;
- To process a magazine subscription;
- To provide [medical, dental, counselling] services;
- To enrol the client in a program;
- To send out association membership information;
- To contact our [clients, customers, members] for fundraising;
- To ensure a high standard of service to our [clients, customers, members];
- To meet regulatory requirements;
- To assess suitability for tenancy;
- To collect and process rent payments;

*[**OPTIONAL ADDITION:** Consider including after each applicable purpose statement the personal information you collect to fulfill that purpose. For example: To verify identity, we may collect name, home address, home telephone number and birth date;]*

Policy 2 – Consent

2.1 We will obtain client, customer, member consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent).

2.2 Consent can be provided [*include the methods that apply to your organization: e.g., orally, in writing, electronically, through an authorized representative*] or it can be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the client, customer, membervoluntarily provides personal information for that purpose.

2.3 Consent may also be implied where a client, customer, member is given notice and a reasonable opportunity to opt-out of his or her personal information being used for mail-outs, the marketing of new services or products, fundraising and the client, customer, member does not opt-out.

2.4 Subject to certain exceptions (e.g., the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate

the performance of a legal obligation), clients, customers, memberscan withhold or withdraw their consent for Name of organization to use their personal information in certain ways. A client's, customer's, member's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide a particular service or product. If so, we will explain the situation to assist the client, customer, member in making the decision.

2.5 We may collect, use or disclose personal information without the client's, customer's, member's knowledge or consent in the following limited circumstances:

[Fill in the situations that may be applicable to your organization. A full listing of such circumstances can be found in sections 12, 15, and 18 of PIPA. Some examples include:]

· When the collection, use or disclosure of personal information is permitted or required by law;
· In an emergency that threatens an individual's life, health, or personal security;
· When the personal information is available from a public source (e.g., a telephone directory);
· When we require legal advice from a lawyer;
· For the purposes of collecting a debt;
· To protect ourselves from fraud;
· To investigate an anticipated breach of an agreement or a contravention of law

Policy 3 – Using and Disclosing Personal Information

3.1 We will only use or disclose client, customer, member personal information where necessary to fulfill the purposes identified at the time of collection [*or for a purpose reasonably related to those purposes such as:*

Fill in any related purposes for which your organization uses or discloses personal information. Examples that may be applicable to your organization, include:

· To conduct client, customer, member surveys in order to enhance the provision of our services;
· To contact our [clients, customers, members] directly about products and services that may be of interest;]

3.2 We will not use or disclose client, customer, member personal information for any additional purpose unless we obtain consent to do so.

3.3 We will not sell client, customer, member lists or personal information to other parties [*unless we have consent to do so*].

Policy 4 – Retaining Personal Information

4.1 If we use client, customer, member personal information to make a decision that directly affects the client, customer, member, we will retain that personal information for at least one year so that the client, customer, member has a reasonable opportunity to request access to it.

4.2 Subject to policy 4.1, we will retain client, customer, member personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

Policy 5 – Ensuring Accuracy of Personal Information

5.1 We will make reasonable efforts to ensure that client, customer, member personal information is accurate and complete where it may be used to make a decision about the client, customer, member or disclosed to another organization.

5.2 Clients, Customers, Members may request correction to their personal information in order to ensure its accuracy and completeness. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought.

*[**IF APPLICABLE:** A request to correct personal information should be forwarded to the Privacy Officer [or designated individual].*

5.3 If the personal information is demonstrated to be inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to which we disclosed the personal information in the previous year. If the correction is not made, we will note the clients', customers', members'correction request in the file.

Policy 6 – Securing Personal Information

6.1 We are committed to ensuring the security of client, customer, member personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

6.2 The following security measures will be followed to ensure that client, customer, member personal information is appropriately protected:

[*Fill in security measures that apply to your organization. Examples may include: the use of locked filing cabinets; physically securing offices where personal information is held; the use of user IDs, passwords, encryption, firewalls; restricting employee access to personal information as appropriate (i.e., only those that need to know will have access; contractually requiring any service providers to provide comparable security measures*].

6.3 We will use appropriate security measures when destroying client's, customer's, member's personal information such as [*Fill in destruction methods your organization employs. Examples may include: shredding documents, deleting electronically stored information].*

6.4 We will continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

Policy 7 – Providing Clients, Customers, Members Access to Personal Information

7.1 Clients, Customers, Members have a right to access their personal information, subject to limited exceptions.

[**OPTIONAL ADDITION**: Fill in exceptions to access that might apply. A full listing of the exceptions to access can be found in section 23 of PIPA. Some examples include: solicitor-client privilege, disclosure would reveal personal information about another individual, health and safety concerns]

7.2 A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. [**IF APPLICABLE:** A request to access personal information should be forwarded to the Privacy Officer [or designated individual]

7.3 Upon request, we will also tell clients, customers, members how we use their personal information and to whom it has been disclosed if applicable.

7.4 We will make the requested information available within 30 business days, or provide written notice of an extension where additional time is required to fulfill the request.

7.5 A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the client, customer, member of the cost and request further direction from the client, customer, member on whether or not we should proceed with the request.

7.6 If a request is refused in full or in part, we will notify the client, customer, member in writing, providing the reasons for refusal and the recourse available to the client, customer, member.

Policy 8 – Questions and Complaints: The Role of the Privacy Officer or designated individual

8.1 The Privacy Officer **or designated individual** is responsible for ensuring Name of organization's compliance with this policy and the *Personal Information Protection Act.*

8.2 Clients, Customers, Members should direct any complaints, concerns or questions regarding Name of organization's compliance in writing to the Privacy Officer. If the Privacy Officer is unable to resolve the concern, the client, customer, member may also write to the Information and Privacy Commissioner of British Columbia.

Contact information for Name of organization's Privacy Officer or designated individual:

Insert Contact Information