Community Social Planning Council

Personal Information Protection Policy for Community Social Planning Council March 2022

Overview

At the Community Social Planning Council ("CSPC"), we are committed to providing our clients with safe and effective services. Providing our services involves the collection, use and disclosure of some personal information about our clients; therefore, protecting their personal information is one of our highest priorities.

While we have always respected the privacy of our clients 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 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 ("Policy"), in compliance with PIPA, outlines the principles and practices we will follow in collecting, storing, and protecting our clients' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our clients' personal information and allowing them to request access to, and correction of, their personal information.

This policy also applies to any programs administered by CSPC and any service providers (i.e., client's social service partners) collecting, using, or disclosing personal information on behalf of CSPC.

The **goals and objectives** of these policies are:

- to establish CSPC's approach to collecting, using, and retaining its clients' personal information,
- to describe security measures and protocols to protect CSPC's clients' personal information,
- to identify and pre-empt potential issues which could affect the confidentiality, integrity, and availability of CSPC's clients' personal information,
- to maintain the standing and reputation of CSPC by upholding responsibilities, and
- to meet legal obligations to effectively manage risk and liability.

The **scope** of this policy is the people, processes, and systems needed for CSPC to deliver its services securely, safely, and effectively.

Definitions

Client – an individual who seeks CSPC programs or services

Client Identification Materials, or **Client ID** – any form of an officially issued, governmental document that conclusively states or confirms information relating to a client's identity, biographical background or details, or other basic information.

Personal Information – information about an identifiable individual, such as name, home address, home phone number, email address, license numbers, place of birth, immigration status, biographic data, appearance, ethnic identity, unique marks, and/or family names and history. Personal information does not include contact information (described below).

Contact information – information that would enable an individual to be contacted in keeping with the services sought, and includes name, position name or title, business telephone number, address, email, or fax number. Contact information is not covered by this policy or PIPA.

Privacy Officer – means the individual designated with responsibility for ensuring that CSPC and any of its programs complies with this policy and PIPA. In our documents we call this role the "Information Security Lead."

Privacy Policy – means this document, and includes any revisions to it from time to time.

Roles and Responsibilities

Key roles and responsibilities for the protection of CSPC's information resources, including personal information of its clients, are listed below:

The Board	• Will review, maintain, approve policies and standards to comply with the privacy policy
Board President, Executive Director, and Director of Operations and Finance	• Will create and submit policies for approval, require compliance, and appoint an Information Security Lead. • Revocation of access rights as a formal and document process
Information Security Lead (Director of Operations and Finance)	• Will be a single point of contact for Information Security issues • Integrate security into the organization's change management plan and project management plan to identify and address information security risk • Provide support, risk assessment and analysis if an incident occurs. • Assist in performing information security activities
Operations coordinator	• Will inform personnel of ongoing and new privacy policy adherence activities and require compliance • Maintain awareness • Employ appropriate controls to reduce risk of disruption of information such as unauthorized or unintentional use or modification
All staff, contractors, and volunteers	• Must comply with policies • Promptly reporting security-related incidents, violations, and inappropriate use • Complete required security awareness training • Personal security
Program Partners	• Have in place appropriate policies and practices to protect shared clients

Policy 1 – CSPC Will Collect Personal Information

1.1. CSPC may collect and keep certain personal information in assisting its clients in applying for, obtaining, and storing client identification materials, specifically each client's

- name,
- home address,
- home phone number,
- email address,
- license numbers,
- place of birth,
- biographic data,
- appearance,
- ethnic or other descriptors of identity,
- immigration status,
- unique physical marks,
- family names and information,
- emergency contact information,
- vehicle description and plate number,
- banking or financial information, and/or
- other personally identifiable pieces of information associated with the client.

1.2. Unless the purposes for collecting the personal information are obvious and the client voluntarily provides their personal information for those purposes, CSPC will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

1.3. CSPC will only collect client information that is necessary to fulfil the following purposes:

- To verify identity;
- To communicate with the client;
- To identify the client's communication preferences;
- To assist the client in applying for identification from governmental or other official sources;
- To assist the client by receiving and/or delivering client identification to the client;
- To assist the client by storing the identification for the client;
- To collect and process payments;
- To ensure the orderly management of CSPC and its programs or projects;
- To respond to emergencies, security issues, or breaches;

- To meet statutory or regulatory requirements; and/or
- To fulfil the requirements of funders and to support program evaluation.

Policy 2 – CSPC Will Obtain Client Consent

2.1 CSPC will obtain client consent to collect, use or disclose personal information (except where, as noted below, CSPC is authorized to do so without consent).

2.2 Consent can be provided to CSPC in writing, by email, by completing a form, through an authorized representative (i.e., a support individual personally accompanying the client). Consent can also be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the client voluntarily provides personal information for that purpose.

2.3 Clients can withhold or withdraw their consent for CSPC to use their personal information in certain ways.

2.3.1 There are certain exceptions, however; and examples of exceptions to a client's ability to withhold or withdraw consent may include, e.g., the personal information is necessary to provide a service, or the withdrawal of consent would frustrate the performance of a legal obligation such as fulfilling a statutory or regulatory obligation.

2.3.2 A client's decision to withhold or withdraw their consent to certain uses of personal information may restrict CSPC's ability to provide a particular service or information, and may not apply retroactively.

2.3.3 If so, we will explain the situation to assist the client in making an informed decision.

2.4 CSPC may collect, use, or disclose personal information without the client's knowledge or consent in the following limited circumstances:

- 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 CSPC requires legal advice from a lawyer;
- For the purposes of collecting a debt; and/or
- To investigate an anticipated breach of an agreement or a contravention of law.

Policy 3 – How CSPC Will Use and Disclose Personal Information

3.1 CSPC will only use or disclose client personal information where necessary to fulfil the purposes identified at the time of collection, or for a purpose reasonably related to those purposes, such as

- To conduct client surveys in order to enhance the provision of our services; or
- To contact CSPC clients directly about information or services that may be of interest.

3.2 CSPC will not use or disclose client personal information for any additional purpose unless CSPC obtains consent to do so.

3.3 CSPC will not sell client lists or personal information to other parties.

Policy 4 – How CSPC Will Retain Personal Information

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

4.2 Subject to policy 4.1, CSPC will retain client personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose, and as required by applicable law.

Policy 5 – How CSPC Will Ensure Accuracy of Personal Information

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

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

5.3 If the personal information is demonstrated to be inaccurate or incomplete, CSPC will correct the information as required. CSPC will consider whether to send the corrected information to any organization to which CSPC disclosed the personal information in the previous year. If the correction is not made, CSPC will note the client's correction request in the client's file.

Policy 6 – How CSPC Will Secure Personal Information

6.1 CSPC is committed to ensuring the security of clients' personal information in order to protect against unauthorized access, collection, use, disclosure, copying, modification, or disposal or similar risks.

6.2 CSPC will implement and follow traditional security measures to ensure that client personal information is appropriately protected:

- locked filing cabinets;
- the use of user IDs, passwords, encryption, firewalls;
- restricting access to personal information as appropriate (i.e., only those that need to know will have access;
- contractually requiring any social service providers that partner with CSPC concerning Client ID to confirm the provision of comparable security measures.

6.3 CSPC will also implement and follow informational and technological security measures to ensure that client personal information is appropriately protected:

- Risk assessment, response, and monitoring including vulnerability testing;
- Compliance with frameworks, and best practices;
- Reporting - logs and audits;
- Governance - strategic alignment with mission and business functions consistent with goals and mission;
- Execution of risk management processes to frame, assess, respond to, and monitor risk to organization assets, individuals, other organizations, and nation;
- Allocation of risk management resources;
- Performance based on outcomes by measuring, monitoring, and reporting risk-based metrics to ensure goals and objectives are achieved;
- Optimizing risk management investments; and
- The requirement to perform periodic risk-based assessments.

6.4 CSPC will audit and periodically update its informational and technological security measures as information threats evolve over time, with accompanying training for its staff as may be appropriate. Information security threats evolve, as will the responsibilities, rights, and duties of CSPC personnel.

6.4.1 CSPC will provide security awareness training to all personnel at induction and at a minimum on an annual basis. Occasional training will be provided on a more frequent basis, if necessary, and / or on a specific security threat.

6.4.2 On an ongoing basis, CSPC will:

- Test and maintain information and technological systems, including hardware and software;

- Apply upgrades and patches to information and technological systems;
- Communicate in advance and after changes;
- Auto-update plugins and monthly tracking and inspection of components; and
- Obtain authorization from the Information Security Lead before data is moved from one place to another.

6.5 All personnel are required to identify and raise potential issues immediately with their supervisor and/or the Information Security Lead. Examples of issues which should be raised include

- System(s) not working as expected (e.g., cannot access data, slow service, missing data, etc.);
- Issue reports from third parties (e.g., service provider, impacted third parties)
- Unexpected or suspicious-looking emails; and
- Unexpected files or data appear or disappear.

6.6 CSPC will use appropriate security measures when destroying a client's personal information such as shredding and deleting electronically stored information.

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

Policy 7 – CSPC Will Provide Client Access to Own Personal Information

7.1 Clients have a right to access their own personal information, subject to limited exceptions (see section 23 of PIPA):

- Solicitor-client privilege;
- Disclosure would reveal personal information about another individual; and/or
- If there are health and safety concerns.

7.2 A request to access personal information must be made in writing, and it must provide sufficient detail to identify the personal information being sought. A request to access personal information should be forwarded to the Information Security Lead or designated individual.

7.3 Upon request, CSPC will also tell its clients how CSPC uses their personal information and to whom it has been disclosed, if applicable.

7.3.1 Except as otherwise allowed under applicable law, CSPC will make the information requested under Policy 7.3 available within 30 business days,

or CSPC will provide written notice of an extension where additional time may be required to fulfill the request.

7.4 Except as otherwise allowed under applicable law, CSPC reserves a right to charge a fee to cover its costs for providing access to a client's personal information. Where a fee may apply, CSPC will inform the client of the cost and request further direction from the client on whether or not CSPC should proceed with the request.

7.5 If a request of a client to access their own personal information is refused in full or in part, CSPC will notify the client in writing, providing the reasons for refusal and the recourse available to the client, if any.

Policy 8 – Questions and Complaints: The Role of the Information Security Lead or Designated Individual

8.1 The Information Security Lead is responsible for ensuring CSPC's compliance with this policy and the Personal Information Protection Act.

8.2 Clients should direct any complaints, concerns or questions regarding CSPC's compliance in writing to the Information Security Lead. If the Information Security Lead is unable to resolve the concern, the client may also write to the Information and Privacy Commissioner of British Columbia.

8.3 Contact information for CSPC's Information Security Lead will be provided to any client of CSPC upon request.

Information Security Lead Name & Email

Barry Hutchinson, Director of Finance and Operations finance@communitycouncil.ca

REFERENCES

- BC Government websites
- PIPA – Personal Information Protection Act