PRIVACY PROTECTION AP 1

INTENT

Sunshine Coast Community Services is committed to safeguarding the personal information entrusted to us by our clients, employees, donors, students, volunteers, Board members, contractors and partners, in accordance with the Personal Information Protection Act (PIPA). This policy outlines the principles and practices we follow in protecting personal information. This policy applies to the Society and to any persona providing services on our behalf. A copy of this policy is provided to any party on request.

RELATED POLICIES/REFERENCES

Personal Information Protection Act (PIPA)

PIPA Guidelines – available from the Office of the Information & Privacy Commissioner of BC website, "A Guide to B.C.'s Personal Information Protection Act – https://www.oipc.bc.ca/**guidance**-documents/1438

PIPEDA – Personal Information Protection and Electronic Documents Act of the Office of the Privacy Commissioner of Canada

POLICY

To effectively carry out its operations, the agency collects personal information from employees, donors, volunteers/students and clients. The agency is legally obligated to protect the privacy of this information, and to develop guidelines about the collection, use and disclosure of personal information on behalf of the agency. In keeping with legislative requirements, the agency follows these guidelines and designates a Privacy Officer to oversee internal compliance and communications and handle any complaints. The Privacy Officer is the Executive Director.

All information that is generated within the agency is private and confidential, and is collected, stored and used for the sole purpose of conducting the agency business. The agency obtains consent to collect, use or disclose personal information from employees, donors, volunteers/students, contractors, Board members and persons served, as required by PIPA guidelines.

Everyone who comes in contact with confidential information respects and preserves that confidentiality, both at work and outside work hours and locations. Individuals who utilize or inadvertently access confidential information in the normal process of performing their job, do not disclose the information to any unauthorized person.

WHAT PERSONAL INFORMATION DO WE COLLECT?

CLIENTS

Only the personal information that we need for the purposes of providing services to our clients, including personal information needed to:

- Deliver requested products and services
- Enrol a client in a program
- Send out Society membership information

This information is normally collected directly from our clients or from other persons with the client's consent or as authorized by law. We inform our clients before or at the time of collecting the information of the purposes for which we are collecting the information.

EMPLOYEES

We collect, use and disclose only the amount and type of personal employee information to meet the following purposes:

- Determining eligibility for employment or volunteer work, including verifying qualifications and references
- Establishing training and development requirements
- Assessing performance and managing performance issues if they arise
- Administering pay and benefits (paid employees only)
- Processing employee work-related claims (e.g. benefits, workers' compensation, insurance claims) (paid employees only)
- Complying with requirements of funding bodies (e.g. lottery grants)
- Complying with applicable laws (e.g. *Canada Income Tax Act*, BC Employment Standards Code, BCGEU contractual requirements)

We assume consent to continue to use and, where applicable, disclose information already collected for the purposes collected. We will inform our employees and volunteers of any new purpose for which we will collect, use, or disclose personal employee information, or we will obtain consent before or at the time the information is collected.

CONSENT

We ask for client consent to collect, use or disclose personal information, except in specific circumstances where collection, use of disclosure without consent is authorized or required by law. If a client is unwilling to provide consent we may not be able to provide certain services. Consent is required in writing by signing a consent form.

USE AND DISCLOSURE

CLIENTS

We use and disclose client personal information only for the purpose for which the information was collected, except as authorized by law. For example, we may use client contact information in an emergency situation.

EMPLOYEES/DONORS/STUDENTS/VOLUNTEERS

It is our policy not to disclose personal information about our employees/donors/volunteers/students without consent. In the case of requests for a reference the only personal information that we would provide without consent is:

- Confirmation that an individual was an employee, student or volunteer, including the position, and date range of the employment or volunteering
- General information about an individual's job duties and information about the employee, student or volunteer's ability to perform job duties and success in the employment or volunteer relationship

PROCEDURES

All employees, donors, volunteers/students

1. Safeguard personal information collected, used, disclosed and disposed of in accordance with the regulations (see Safeguarding below).
2. Report any alleged breaches of confidentiality to their supervisor. If an employee is proven to have breached confidentiality, he/she will be disciplined, up to and including termination.
3. Store confidential documents destined for disposal in a safeguarded area in their office. Comply with directions regarding boxing and disposal by shredding.
4. Release confidential information regarding clients on a strictly "need to know" basis to authorized family members and/or any person directly involved in the client's care. This is done with the client's written consent, or the written consent of the client's Representative. If the client or Representative is unable to provide such consent, it may be done only if it is in the best interest of the client.
5. Direct enquiries from the media to the Executive Director or designate.
6. Direct enquiries about information they are not authorized to release to their Supervisor.
7. Sign an Oath of Confidentiality. This is signed during the orientation process and remains in effect throughout the employment period and after termination.

Executive Director, Management Team and Designates

1. Ensure that employees receive appropriate orientation and training regarding privacy and confidentiality.
2. Provide appropriate systems and instructions to ensure secure storage of confidential information.
3. Arrange for secure disposal, by shredding, of confidential information no longer required. This is done approximately four times a year.
4. Provide opportunities for clients and employees to learn about their rights regarding their personal information, including the right to review and correct it.
5. Promptly document and investigate any reported or alleged breaches of confidentiality; report to Privacy Officer and include allegations and investigations in the annual Compliance Report.

Executive Director

1. Appoints a member of the Management Team to act as the agency Privacy Officer, as prescribed in the Personal Information Protection Act (PIPA).

The Agency Privacy Officer

1. Ensures the agency compliance with PIPA.
2. Communicates the requirements of PIPA within the organization.
3. Responds to employee, volunteer/student and client requests for access to personal information.
4. Addresses general issues concerning personal information.

SAFEGUARDING OF PERSONAL INFORMATION

COLLECTION, STORAGE AND DISPOSAL OF PERSONAL INFORMATION

Electronic Files:

1. Personal information stored in an electronic format will be safeguarded in accordance with the security measures outlined in the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada

2. Computers are password protected and staff must log in to input or access personal information.
3. No personal information will be collected beyond what is necessary or appropriate for the organization's purpose.
4. Personal Information is accessible only to those who use it or on a need to know basis.
5. Computers are physically secured, backed up regularly to a secure location, and doors are locked.
6. Firewalls (hardware and software) and anti-virus software are installed and are updated regularly to protect computers against invasive malware.
7. Networks have adequate encryption according to current encryption standards.
8. The use of removable drives, USB flash drives, and portable electronic devices for the purpose of storing personal information is **strictly prohibited** unless with the express authorization of the Executive Director or their designate. Where approved, the mobile drive must be password protected and encrypted and all files contained therein must be uploaded to the secure electronic system at the first possible opportunity.
9. Disposal of electronic files is conducted in accordance with PIPEDA guidelines. Electronic media storing personal information is either destroyed or reformatted to prevent data recovery.

Physical (Paper) Files

Where working files and original documents must be retained in paper format they will be kept as outlined below:

1. Personal information not stored in an electronic format is stored in locked filing cabinets within locked offices.
2. All documents containing personal information including client related information must be removed from the desk top at the end of each day and stored in locked cabinets.
3. Keys are secured and access to files is limited to persons authorized by the SCCSS and on a need know basis.
4. Persons required to travel with working files containing personal information will ensure they are properly stored, always on their person and at no time left in vehicles or other such locations for the duration of their use.
5. Physical files containing personal information will be securely retained for a period of time determined by applicable legislative requirements, or for a reasonable amount of time in the absence of legislative requirements as deemed appropriate by the Society.
6. Physical files and documents will be destroyed using on-site shredders or secure third-party contractors as required.

ACCESS TO PERSONAL INFORMATION

Clients

1. Individuals have the right to review and correct where necessary personal information collected by those working on behalf the Society.
2. Upon written request to the Executive Director or their designate, information pertaining to the individual will be provided to that individual within 30 days.
3. Requests can be sent to the Society email address privacy@sccss.ca. When the complainant is unable to provide the details in writing or by email, reasonable accommodation to obtain the details of the complaint verbally will be made.

Employees/Students/Volunteers
These files may be accessed with two days' written notice – refer to policy HR B5.

COMPLAINTS RESOLUTION PROCESS

From time to time concerns may arise that require further assistance and review. Individuals who feel their personal information has been compromised with respect to the Society's *Protection of Personal Information Policy and Procedures* are encouraged to deal with concerns through the following complaint resolution process:

1. Written complaints outlining concerns about any collection, use or disclosure of personal information should be sent to privacy@sccss.ca. When the complainant is unable to provide the details in writing, reasonable accommodation to obtain the details of the complaint verbally will be made.
2. A representative designated by the Society will contact the complainant within seven calendar days to obtain further details.
3. The representative will review the facts and circumstances surrounding the complaint including interviewing other parties when necessary.
4. The representative will inform individuals of the outcome of the review and of any relevant steps taken in writing and within 30 days.
5. The representative will also inform the complainant of their right to complain to the Office of the Information and Privacy Commissioner if they are not satisfied with the Society's response to their complaint. Relevant contact information shall also be provided to the complainant.
6. Where the complaint is justified, the Society will take appropriate measures to rectify the situation including changes to the policy and procedures as well as communicating those changes to relevant staff.
7. The Society will follow up to verify that required changes to policies, procedures or practices have been undertaken.

INCIDENT HANDLING

The Society is obligated to report all suspected or confirmed incidents of misuse of personal information immediately to the Office of the Information and Privacy Commissioner in accordance with PIPA using the following process:

1. As soon as the incident is suspected or known, employees are required to immediately report any incidents to their manager who will advise the Executive Director or designate.
2. The Society immediately reports the incident to the Office of the Information and Privacy Commissioner and when applicable, the service contract designate.
3. The Executive Director or designate is the sole contact for questions or calls from the media, public or funders. All efforts will be made to contain the information and to determine foreseeable harms and/or risks to individuals.
4. On an urgent priority basis, the Society's designate will review the circumstances of the incident and arrange for representatives to advise affected individuals/clients of the suspected or known incident as soon as possible and brief the Office of the Information and Privacy Commissioner.
5. The Office of the Information and Privacy Commissioner will initiate an investigation and direct remediate and preventative actions as required.

6. Employees, who fail to take reasonable safeguards to protect personal information obtained in the course of their employment with the Society, may be subject to disciplinary action as per HR Policy D4 or in accordance with the relevant collective agreement.

Definitions

Personal Information: means information about an identifiable individual. This includes but is not restricted to: an individual's name, home address and phone number, age, gender, marital or family status, an identifying number, financial information, educational history, etc. It also includes information whose unauthorized disclosure could be prejudicial to the interests of the agency and/or individuals in or associated with the agency. This includes personal plans and reports regarding the health, goals, needs and services of clients, and employment information about employees such as Social Insurance Numbers and performance reviews.

Confidential Documents: include any document, in written, audio, photographic or video format, that contains confidential information. This includes, but is not limited to:

a) All documents containing personal information about clients and families, such as name, address, date of birth, medical reports, service needs etc.
b) Any document containing personal information about an employee, or related to an employee's performance or to a disciplinary matter.
c) Incoming and outgoing faxes/e-mails marked confidential

Breach of Confidentiality: is an action or omission that results in confidential information being shared with an unauthorized person. Examples of breaches of confidentiality include, but are not limited, to:

a) Disclosing confidential information obtained on the job to any unauthorized person.
b) Deliberately accessing confidential information not needed for performing the job, whether or not that information that information is disclosed to another person.
c) Discussing a client's or co-worker's personal information casually with another employee.
d) Disposing of confidential documents without shredding them
e) Keeping client and employee records unlocked or allowing unauthorized individuals to have access to those records.
f) Commenting to requests from the media regarding the agency affairs, rather than referring the media to the Executive Director.

Notes:
PIPA Guidelines
Form: Oath of Confidentiality

EFFECTIVE: December 1, 2015	**APPROVED BY: Executive Director**	
REPLACES: April 1, 2014	**MONITORING: ED and MT**	**FREQUENCY: Annually**