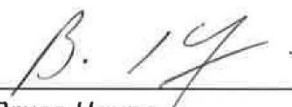




SECTION 4: PRIVACY

Authorization of policies contained in Section 4: Privacy

The signature affixed below indicates that the policies and procedures contained in this section of the Sources Policy Manual have been reviewed and authorized by the Board of Directors of Sources Community Resources Society on the date indicated.



Bruce Hayne
Board President



Date of Authorization

TABLE OF CONTENTS

4. PRIVACY	4
4.1 Statement and Purpose.....	4
4.2 Accountability	4
4.3 Purposes for Collection, Use and Disclosure	4
4.3.1 Employees and Applicants.....	4
4.3.2 Volunteers	4
4.3.3 Clients.....	5
4.3.4 Board and Society Members.....	5
4.3.5 Donors.....	5
4.4 Access to Personal Information (Revised 2017).....	5
4.5 Disclosure of Information to Third Parties (Revised 2015).....	6
4.6 Consent to Collection, Use and Disclosure (Revised 2017).....	7
4.7 Limiting Collection	8
4.8 Limiting Use and Disclosure.....	8
4.9 Retention and Destruction of Files	9
4.9.1 Information Used to Make a Decision About a Person.....	9
4.9.2 Client Files (Revised 2015).....	9
4.9.3 Destruction of Files (Revised 2011).....	9
4.10 Accuracy of Information (Revised 2017)	10
4.11 Safeguards (Revised 2015)	10
4.12 Web-based Technologies and Electronic (Revised 2015).....	11
4.12.1 Compliance.....	11
4.12.2 Data Ownership.....	11
4.12.3 Data Confidentiality Levels	11
4.12.4 Passwords.....	12
4.12.5 Securing Computers that are Not in Use.....	13

4.12.6	Security While Off-Site.....	14
4.12.7	Electronic Transmission of Confidential Information (Revised 2015).....	15
4.12.8	USB and Other Data Storage Devices	15
4.12.9	Equipment and Data Disposal.....	16
4.12.10	System Backups.....	16
4.12.11	Confidentiality/Security Breaches.....	16
4.12.12	Website and Social Media (2015).....	17
4.13	Communication of Policies and Procedures	17
4.14	Compliance (Revised 2017)	17

4. PRIVACY

4.1 Statement and Purpose

Sources respects and upholds an individual's right to privacy and protects personal information. Personal information is information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Sources is committed to ensuring compliance with applicable privacy legislation.

4.2 Accountability

Sources is accountable for the personal donor, client, member, employee, and volunteer information under its control. This includes personal information that is transferred to third parties for processing, storage or other purposes.

The Privacy Officer, in cooperation with the Senior Management Team, is responsible for the organization's compliance with this Policy.

4.3 Purposes for Collection, Use and Disclosure

Sources collects and uses personal information about donors, clients, members, employees and volunteers for a variety of purposes, as specified below. Purpose for collection is identified before or at the time the information is collected.

4.3.1 Employees and Applicants

Employee and applicant information is collected and used for contact purposes as well as to administer compensation, benefits and pension programs. Information collected is also used to make decisions with respect to hiring, dismissal and performance evaluation.

4.3.2 Volunteers

Information collected on volunteers is used to contact the volunteer, make decisions regarding assignment and dismissal and to complete performance reviews.

4.3.3 Clients

Information about clients is collected and used to contact the client, to determine eligibility for services, to deliver services, assess progress and promote the safety of the individual, other clients and/or staff.

Also see Section 6.1: Client Files.

4.3.4 Board and Society Members

Information collected from board and Society members is used only for the purpose of contacting the individual.

4.3.5 Donors

The collection of donor information is limited and used only for the purpose of processing donations to the Society.

4.4 Access to Personal Information **(Revised 2017)**

All persons for whom personal information is stored by Sources have the right to access their personal information under the Personal Information Protection Act and/or the Freedom of Information and Protection of Privacy Act. The Privacy Officer will assist with access requests.

Unless prohibited by law, Sources provides the persons served access to their own files, **to information about the ways in which their information is or has been used, and the names of the individuals and organizations to which their personal information has been disclosed**

- Minor children under thirteen (13) years of age may have access if requested by a parent or guardian and must be accompanied by them for viewing the file.
- Minor children thirteen (13) years of age or more may request access on their own.
- Where the service has involved the family group, every effort will be made to have all parties agree to review the information together. When that is not possible, only information about the person accessing the file will be released to them (1999).

Request for access must be made in writing to the appropriate Sources Program

Manager who will provide requested personal information within 30 business days after it is requested or will give written notice if it needs more time to respond.

Sources may request clients to prove their identity before giving them access to their personal information. All third party information will be removed under the direction of the Privacy Officer prior to the file being reviewed. Files are to be reviewed at a Sources site in the presence of professional staff unless third party information is removed and the severed file copied for the client to take away (1999, Revised 2008). Any personal information that is stored electronically must be printed. Direct access to electronic files is strictly prohibited.

Closed files stored off-site may be accessed only by the Senior Management Team.

In certain exceptional situations, Sources may not give an individual access to certain personal information, where authorized or required by the Personal Information Protection Act (PIPA) to refuse access. In the case of client files, Sources only refuses to share sensitive information where it is believed that the sharing of the information will cause harm to the client. The decision to withhold information must be reviewed and approved in writing by the Chief Executive Officer (1995). Where access cannot be provided, Sources will provide written notification of the reasons for the refusal to the client (also entered into the case record) and outline further steps that are available to the applicant. For example, a qualified professional, having signed a written statement indicating that sensitive information will not be divulged to the client, may be appointed to review the file on behalf of the client (2003, Revised 2008). **The client also has the right to ask the Office of the Information and Privacy Commissioner for British Columbia to review the decision**

4.5 Disclosure of Information to Third Parties (Revised 2015)

Open and closed files are routinely accessed only by Sources staff and volunteers who are or were working with the person whose record is being examined. This may include direct services staff assigned to the case, the Program Manager, clerical staff, a volunteer or a practicum student (1990, Revised 1995).

Other access is for supervision and/or quality improvement (1999). Sources allows access to records to professionals who must examine files for program auditing, licensing, legal or accreditation purposes. The person examining the files must come from a reputable governmental or professional agency which abides by an oath of confidentiality. Third party access to files is only permitted with the written

authorization of the Chief Executive Officer (1990).

The only circumstances under which personal information may be disclosed to third parties is for the fulfillment of any purposes identified above, or as required by law. All release of information is done in accordance with the Personal Information Protection Act. If a program is federally funded, the Freedom of Information and Protection of Privacy Act takes effect.

Prior to releasing personal information to a third party, Sources determines if the reason to release information is valid (i.e. justifiable, legitimate, legally permissible, and in the best interest of the client). As needed, Sources obtains legal counsel to determine conditions under which client records may be released. If the reason is determined to be valid, Sources obtains informed written consent from the client (or their parent/guardian), the employee or volunteer. If the person served is a minor in the care of the Ministry for Children and Family Development, consent must be obtained from the child's social worker. In the case of an adult with a developmental disability who cannot understand the consent, consent must be obtained with the assistance of a family member or advocate who knows the client well or the client's social worker. Plain language is to be used, the consent read aloud or an interpreter used where understanding is compromised (1999).

Consent must indicate what information is to be disclosed, to whom, by whom and the reason for the disclosure. Consent must be obtained each time information is to be released and indicate the date the consent takes effect as well as the expiry date of the consent (rev. 2002). For one time releases of information, expiry must not exceed 90 days from the date consent is given. When the release of information is required for ongoing service provision, expiry must not exceed 1 year from the date consent is given (2006). The client maintains the right to revoke consent at any time (rev. 2002). Copies of signed release forms are provided to the client. Originals are placed in the case record.

When permitted or required by law, regulation, or court order, confidential information may be released without the authorization of the client or legal guardian. However, the client or legal guardian will be informed that the information will be released.

4.6 Consent to Collection, Use and Disclosure **(Revised 2017)**

Sources obtains consent for collection, use and disclosure of all personal information.

There are two types of consent: Expressed and Implied. The following is the definition of Expressed and Implied consent:

Express consent is permission for something that is given specifically, either verbally or in writing. It is required to collect, use or disclose sensitive personal information such as medical data or personal financial information. Verbal consent is to be verified by an independent 3rd party or with a complete and unedited audio recording. Written consent can be paper-based or electronic i.e. checking a box on the website.

Implied consent is defined as an assumption of permission that is inferred from actions on the part of the individual. Implied consent also entails publically available information or if a recipient voluntarily discloses their contact information without indicating they don't want to receive communications. Sources may use implied consent to collect, use or disclose personal information where one or more of the following apply:

- A client relationship already exists;
- Express consent has previously been given; or
- Where the purpose of using the personal information is apparent.

Persons having given consent may change or withdraw consent at any time (subject to contractual or legal restrictions and reasonable notice) by contacting the Program Manager or Director.

4.7 Limiting Collection

Sources collects only the information required to meet the needs and obligations outlined in Section 4.3.

Sources will collect personal information only by clear, fair and lawful means.

4.8 Limiting Use and Disclosure

Sources will not use or disclose personal information for any purpose other than those for which it was collected, except with consent or as required by law.

If personal information is disclosed to third parties (for the fulfillment of any purposes identified in 3.3), Sources will ensure that appropriate security undertakings, such as

confidentiality clauses in contractual agreements, are employed to protect the transfer and use of personal information.

Sources does not sell, trade or rent information to third parties.

4.9 Retention and Destruction of Files

Sources retains personal information only as long as it is required for the identified purpose(s) or as required by federal and provincial law.

Psychologists and other counselling professionals may be subject to additional retention/destruction obligations under legislation or regulations applicable to their respective governing bodies.

4.9.1 Information Used to Make a Decision About a Person

Sources retains personal information for a minimum of one year where that information is used to make a decision that directly affects the individual (e.g. application for service or job candidate).

4.9.2 Client Files (Revised 2015)

Client files are kept for a basic seven year retention (rev. 2002). Files of clients under the age of nineteen (19) must be kept for seven years after the age of majority. Files which are deemed property of the funding agency should be returned to the funder as per the funder's instructions.

Upon completion or closing of the contract and upon written authorization from the Province of British Columbia, Sources is required to dispose of any electronic copies they may have via an IT professional.

4.9.3 Destruction of Files (Revised 2011)

Sources destroys its documents containing personal information as soon as it is reasonable to assume that:

- a. The purpose for which that personal information was collected is no longer being served by retention of the personal information; and

- b. Retention is no longer necessary for legal or business purposes. Legal considerations include consultation with legal representatives of clients for whom files are maintained.

Files of programs that operate under contract with provincial or federal government agencies must follow destruction procedures of those agencies. Files should not be destroyed without written authorization of the government agency.

Sources employs a system of periodic records review, in order to evaluate whether there remains a purpose for retaining the personal information in the records. If there is no such purpose, the personal information is destroyed.

In the event of dissolution of the organization, files of programs that operated under contract with government agencies will be forwarded to those agencies. Files of programs not operating under government contracts will be destroyed in a confidential manner.

4.10 Accuracy of Information **(Revised 2017)**

Sources will maintain personal information up-to-date, accurate and relevant for its intended use. **Individuals may write to ask to correct any errors or omissions in their personal information. If the individual's request for correction is considered reasonable, the personal information will be corrected as soon as reasonably possible. Sources will, as soon as reasonably possible, also send the individual's corrected personal information to each organization it was disclosed to during the year before it was corrected. If Sources does not correct an individual's personal information, the requested correction will be noted on copies of the personal information.**

4.11 Safeguards (Revised 2015)

Sources will protect personal information with appropriate security safeguards including physical, administrative and electronic security measures.

Access to files or documents containing personal information is limited to authorized personnel on a need-to-know basis. These documents must not be left unattended at any time (e.g. on a desk) and are stored in locked cabinets, accessible only to authorized program personnel (2006).

4.12 Web-based Technologies and Electronic (Revised 2015)

Web-based technologies and electronic communications include, but are not limited to, the organization's own website, email, external websites, blogs, social media and networking sites, wikis, discussion forums, and photo and video sharing sites where the organization's staff and volunteers may interact with each other or with service recipients.

This procedure applies to all IT related equipment, processes, and data that belong to Sources, or is managed on its behalf, wherever accessed.

4.12.1 Compliance

All members of Sources, affiliates, and third-parties will comply with this IT security procedure and, where appropriate, their compliance will be monitored.

4.12.2 Data Ownership

All data collected, recorded, and produced by Sources is owned by Sources. Sources data may not be used for purposes other than that for which it was originally intended without approval by the Chief Executive Officer or designate.

4.12.3 Data Confidentiality Levels

The security procedures that are appropriately applied to a given set of information will depend on the characteristics of that information. It is important, therefore, to have a classification scheme that indicates the level of protection that must be applied.

a. Sensitive

Sensitive information is to be accessed by a strictly controlled group of users, with owners' consent, and with highest security levels applied. This information is not to be passed on without consent and is subject to the Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Information Protection Act (PIPA), and/or Freedom of Information and Protection of Privacy Act (FOIPPA) as appropriate to the nature of the Society's contract with the individual. Examples of sensitive information include medical, criminal, or financial information of a personal or business critical nature.

b. Confidential

Confidential information is personal information about an individual (e.g. name, home address, phone number, date of birth) and is to be kept secure and accessed only for Society business. It is to be passed on to third parties only with consent and only as required for the fulfillment of the Society's contract with the individual. Confidential information is also subject to privacy legislation (PIPEDA, PIPA, and/or FOIPPA).

c. General

General information does not contain any personal information and is not restricted other than by section 10.4 of this policy manual, which permits only the Chief Executive Officer (or designate) to comment publicly on the affairs of the Society.

4.12.4 Passwords

Passwords are the key to many systems and applications. A password helps to prove identity, ensure personal privacy and helps protect the security of the data being accessed.

a. Strong Passwords

A strong password is one that is difficult to guess. It will use a wide range of characters in an unpredictable order.

A password must be at least eight characters long and must use a mixture of at least three of the following four characteristics:

- Upper case letters;
- Lower case letters;
- Numbers; and
- Punctuation characters.

Sources policy ensures secure passwords by implementing a system that will not allow a less than strong password to be used; that does not allow the 'save my password' feature; and that requires strong passwords to be reset every 90 days.

b. Password Security

Additional password security requirements are as follows:

- A good password is one that can be remembered easily and typed in quickly so that others within viewing range are not be able to distinguish the password.
- Passwords must not be displayed on screens as they are entered. As an added precaution, the password display feature is inactive for all Sources devices.
- Passwords do not need to be tracked in case they are forgotten. They can be reset by the IT contractor.
- Passwords must not be disclosed to anyone other than the direct supervisor or system administrator.
- When allocated a new or temporary password, the user must immediately change it.

4.12.5 Securing Computers that are Not in Use

When a computer is left unattended, it is essential that no unauthorized person can gain access to it. Sources staff must use one of the following techniques:

a. Log Out

Logging out will prevent any access until an authorized user enters their username and password.

b. Lock the Keyboard

Locking the keyboard will prevent any access until the current user re-enters his or her username and password. To lock the keyboard, the user must press Ctrl/Alt/Delete and select the 'lock' option. To unlock the computer, the user must press Ctrl/Alt/Delete again and re-enter his or her username and password. The computer will resume from the point at which it was locked.

As an added protection, Sources computers automatically lock after ten minutes of inactivity.

Note: The lock option prevents any other user from accessing the computer. Only the user that locked the computer is able to unlock it.

c. Shut Down

Shutting down the computer should not be used unless using a notebook (portable) computer. Shutting down prevents automatic updates that are critical to the functioning and security of the entire system.

4.12.6 Security While Off-Site

There are several additional checks that must be performed when a mobile data-carrying device (such as a notebook or smartphone) is used.

Any data of value to the organization must be placed on secure agency storage by accessing the agency server through remote access or, if an internet connection is not available off-site, immediately on return to the program. Once the data is saved on the server, it must be erased from the device memory.

a. Notebook Security

Notebook security is the responsibility of the user. Notebooks must be securely locked away when not in use and must not be left unattended in a public place or in a vehicle.

b. Software Security

Users of agency-owned notebooks must not install any unapproved software. This applies to software downloaded from the internet; unlicensed or illegal software; or software obtained from any other source. Advice on installing additional software can be obtained from a technical consultant.

c. Virus Protection

All agency-owned notebooks must have approved security software which includes, as a minimum, anti-virus and anti-spyware components. The anti-virus software must be updated regularly, each day preferably, but at least once a week by connecting the notebook directly to a network connection.

d. Password Security

All portable computing devices that contain agency information must be password protected.

e. Off-Site Access to Data

When accessing data via remote connection – whether at home, on another computer, or in a public place – users must ensure that:

- Sensitive or confidential information is secured by the use of passwords or file encryption;
- Information is not divulged to any family members or to anyone else outside the agency;
- Up-to-date anti-virus and anti-spyware software is used; and
- The connection is closed immediately after use.

4.12.7 Electronic Transmission of Confidential Information (Revised 2015)

Personnel who deliver services using electronic media, including telephone and computer, discuss associated risks with service recipients.

a. Sources Email System

Sources personnel must use only the Sources email systems for agency related emails.

b. Incoming Messages

When using email, personnel must not open messages or attachments that are unexpected or from unknown sources.

c. Outgoing Messages

The greatest cause of email exposure of confidential or sensitive data is sending email to the wrong recipient. Personnel must carefully check all addresses before sending messages and must include a standard privacy message in their email signatures.

4.12.8 USB and Other Data Storage Devices

USB and other data storage devices are permitted for temporary storage of general Sources data only. Data classified as sensitive or confidential (see data confidentiality levels above) may not be stored on portable data storage devices unless authorized by the Chief Executive Officer.

4.12.9 Equipment and Data Disposal

The agency has introduced an environmentally-responsible procedure for the disposal of all electronic equipment. In relation to the disposal of IT equipment, a secure data erasure procedure has been integrated into the process. This procedure applies to PCs, printers, hard drives, USB memory sticks, and any other devices that may potentially contain data.

Data on such devices may contain sensitive or confidential data and must never be thrown away or given away. Equipment must be given directly to the IT contractor for all data to be located and erased. If the equipment is to be reused within the agency (i.e. transferred to another individual or program), the data will be erased and the software prepared for the new user. All other hardware will be recycled by the IT contractor.

4.12.10 System Backups

System backups play an important role in ensuring business continuity in the event of an IT equipment or software failure by providing a method of restoring systems to pre-failure state.

Backup of Sources' server data is conducted by the IT contractor. Information stored on individual devices is not backed up; therefore staff must store all agency information on the agency servers.

4.12.11 Confidentiality/Security Breaches

All incidents which result in a loss of hardware or a security breach must be reported immediately to the appropriate Director. The Director and Privacy Officer will investigate the incident and determine the security threat resulting from it.

Reportable incidents include but are not limited to:

Loss/theft of hardware;
Loss/theft of software/data;

Unauthorized access;
Misuse of system/privileges; and
Illegal software download.

4.12.12 Website and Social Media (2015)

Sources Privacy Policy is posted on the agency website. Visitors to the agency's website or social media forums can be assured that any information collected by Sources will not be misused.

4.13 Communication of Policies and Procedures

Sources is committed to providing understandable and easily available information about our privacy policy and practices. This policy and related information is available at all times on our website, www.sourcesbc.ca.

4.14 Compliance (Revised 2017)

Sources will respond in a timely manner to questions, concerns and complaints about our privacy policies and procedures. Correspondence of this nature may be directed to the Privacy Officer at rsidhu@sourcesbc.ca. **Individuals who are not satisfied with Sources' response can complain to the Office of the Information and Privacy Commissioner for British Columbia.**