CONFIDENTIALITY AND PRIVACY POLICY

POLICY

Family Service Toronto (FST) protects and respects the confidentiality of all information entrusted to the organization, except as permitted or required by law or contract, and in accordance with all municipal, provincial and federal legislation.

The following is considered confidential information:

- All matters/documentation relating to clients.
- All contracts.
- All Human Resources files and proceedings.
- All financial information, status and statements.
- All information or documentation labelled "Confidential" by the organization, or listed as such by separate memorandum, or e-mail that advises confidential status.
- Any information pertaining to FST's donors or members.

This information may be related to, without being limited to, personal information of any kind about clients or employees, students, volunteers, donors or members as well as information about the operations of FST (e.g., personnel matters, internal financial procedures, contractual information, and intellectual property of FST).

Respect for the organization's confidentiality and privacy policy is of utmost importance.

Confidential information shall not be used for any purpose other than its reasonable use in the normal performance of employment duties.

SCOPE

This policy applies to all FST personnel (employees, students, volunteers).

REQUIREMENT OF CONFIDENTIALITY

In accordance with PHIPA (Personal Health Information Act), FST requires all employees to handle sensitive personal client information in a confidential and appropriate manner. It is understood that employees of FST will become aware of confidential information regarding our clients through the course of their employment. Employees, students and volunteers agree that if confidential information is not effectively protected, the operations of FST may be threatened, and the well-being and privacy of our clients may suffer irreparably.

Employees, students and volunteers will take all reasonable precautions to safeguard the confidentiality of such information (e.g., ensuring confidential material is kept locked when not being used; shielding computer screens with confidential information from unauthorized viewing; taking special precautions when transporting confidential documents).

PRIVACY STATEMENT

FST collects, uses, and shares personal information about our clients, donors and members in order to:

- Provide quality programs and services to clients.
- Provide information to other people or organizations with client consent (for example, making a referral for service).
- Contact clients, donors and members to evaluate FST's service and work.
- Conduct research
- Contact individuals about our fundraising and membership activities
- Recognize donor contributions
- Report to funders and others as required
- Review client files to ensure high quality of service and documentation.

FST may also collect, use and share personal information with consent or as permitted or required by law or contract.

CLIENT PRIVACY

FST is committed to protecting the privacy of its clients and ensuring that:

- the personal information it receives from clients is kept safe, secure, confidential, accurate and up to date
- clients understand why their personal information is collected by FST
- FST obtains client consent before collecting, using, sharing or releasing client information, except as set out in this policy or permitted or required by law or contract
- only the personal information necessary for the purposes listed above is collected from clients, unless otherwise consented to by the client or permitted or required by law
- access to client information is limited to the FST employees, volunteers and students involved in delivering services to clients
- any external agents to whom FST releases information have a need to know and only use and disclose client information for the purposes for which it was originally provided
- clients can withdraw their consent at any time to the collection, use and disclosure of their personal information
- clients have access to their record, except where FST is entitled to refuse an access request, and are able to copy or correct their record and ask questions about FST's privacy policies and procedures
- complaints about FST's privacy policies and procedures are handled efficiently and effectively
- all legal and regulatory requirements regarding client information are met and maintained.

Only a person who provides a provincially funded health resource to an individual may require the individual to produce his or her health card. FST personnel may ask clients to voluntarily provide their health card number to facilitate referrals to provincially funded health resources.

PROCEDURES

1. Obtaining Consent for the collection, use and disclosure of personal information

1.1 As FST services often involve collaboration and consultation among employees. FST employees will discuss the following with new clients:

- the nature and extent of consultation and collaboration in the FST program or service which the new client is accessing
- the personal information that FST may collect
- the purposes for which FST collects, uses and shares personal information, as listed above.

1.2 Client's rights and responsibilities including rights related to keeping client's personal information private will be reviewed with all new clients at their first appointment following intake.

1.3 Clients will be asked to sign a form indicating that the organization's privacy policies have been discussed and that the client consents to the collection, use and sharing of personal information for the purposes listed in this policy.

1.4 The signed forms will be scanned to the client's file, and the original copy consent will be destroyed.

1.5 In cases where it is not possible or practical to obtain the client's written acknowledgment (e.g., virtual service), the documents will be sent to the client for review and return via email with a statement that the client has reviewed and agrees to the content of the acknowledgement form. Where this is not possible (e.g., client can not access documents electronically or where accommodations are required, verbal acknowledgment that the organization's privacy practices have been explained to, and accepted by, the client will be recorded in an activity note in the client's record.

1.6 Consent will be that of the individual and must be knowledgeable, relate to the personal information and not be obtained through deception or coercion. A consent to the collection, use or sharing of personal health information about an individual is knowledgeable if it is reasonable in the circumstances to believe that the individual knows, (a) the purposes of the collection, use and/or disclosure, as the case may be; and (b) that the individual may give or withhold consent.

1.7 In the event that employees are concerned that a client does not have the capacity to consent to the collection, use and disclosure of his or her personal information, employees should refer to the *Addressing Concerns About Client Capacity* policy and document concerns within the client file.

2. Client Withholding, Limiting or Withdrawing Consent

2.1 Clients are informed of their responsibility to provide relevant information as a basis for receiving services and participating in service decisions.

2.2 Clients have the right to stipulate who will have access to their personal information. This means that they can withhold, limit or withdraw their consent to the collection, use or disclosure of personal information. The request may cover all or a specific part of a client's record. When this happens, staff will implement the following "lock-box" procedure.

Electronic records: The FST employee receiving the client's request to withhold, limit or withdraw their consent will:

- Record the verbal instructions by the client in an activity note in the client's electronic record and/or scan any written instructions by the client into the client's electronic record.
- Notify the Information Technology (IT) Department or their designate of the client's instructions and the IT Department will activate the lock box in the electronic client records in accordance with their request (e.g. partial or full locking of the record)

2.3 In cases where the withholding, limiting or withdrawal of consent will limit or prevent FST from continuing to deliver services, employees will discuss with the client the consequences of their withholding, limiting or withdrawal of consent.

3. Higher Levels of Confidentiality (Use of Aliases)

3.1 FST serves clients periodically that require a higher level of confidentiality. For example: public figures; employees of a fst funder; former personnel who may not wish it to be known that they are accessing fst services.

3.2 In such situations, programs will provide clients an opportunity to select and use an alias. The alias will be used in the client record and in the client's interactions with fst.

3.3 In the event a client requests an alias, they will be directed to fst's privacy officer. No other personnel may create an alias in the database.

3.3 A list of the aliases, clients' real names and file numbers will be confidentiality maintained outside of the client database by the fst privacy officer.

3.4 A higher level of confidentiality designation does not invalidate the normal legal limits to confidentiality, which includes subpoenas, search warrants and the right of government funders to audit client records. Clients will be informed of these limitations on confidentiality by fst's privacy officer

3.5 The human resources department will provide names of new personnel to the fst privacy officer so that a check of the client database can be completed. If the individual has received service from fst in past, an alias will be assigned to the record in order to maintain their privacy.

4. Disclosure without Consent Including Responding to Summons/ Subpoenas/Court Orders and Requests from Police

4.1 FST will not disclose the personal information of clients without their consent, except where:

- It is believed the client or someone else is in imminent danger of serious physical harm (see *Duty to Warn* policy)
- A child under the age of 16 is at risk of or has been abused or neglected (see *Child Abuse Reporting and Documentation* policy)
- FST is subpoenaed or is otherwise served with a court order, summons, warrant or a similar requirement issued by a person who has jurisdiction to compel the production of information in a proceeding (such as a proceeding held in, before or under the rules of a court, a tribunal, a commission, a justice of the peace, a coroner, a committee of a College within the meaning of the *Regulated Health Professions Act, 1991*, a committee of the Ontario College of Social Workers and Social Service Workers under the *Social Work and Social Service Work Act, 1998, a person authorized by statute* or an arbitrator) or
- It is otherwise permitted or required by law or contract.

4.2 If a FST employee, student or volunteer is served with a warrant, summons, subpoena, production order or similar requirement issued in a proceeding, the individual must immediately notify their supervisor, who will provide advice and direction as to how to respond. Dependent on the situation, FST may choose to seek legal counsel. This decision will be made by the supervisor of the program in consultation with the individual and the Director of the program area. FST's Privacy Officer may also be consulted. If a manager, director and/or the Privacy Officer determine that FST should seek legal counsel for the purposes of discussing the situation and/or facilitating access to FST's legal counsel. FST personnel shall follow the same procedure in response to requests by police officers for client information.

4.3 In general, where an order, summons, warrant, subpoena, production order or other requirement to produce documents has been served on FST, FST will:

- make every attempt to respond in a way that is respectful of the order or other requirement, while at the same time taking steps to preserve the client's right to confidentiality
- make an exact copy of the file to remain at FST and
- deliver the documents to the court or other proceeding in a sealed enveloped marked "private and confidential" or via another means arranged by the requestor of the record

4.4 Where FST discloses personal information without the client's consent, the client will be notified of such disclosure as soon as reasonable, practical, safe and/or legally possible in the circumstances.

5. Release of information to third parties with client consent

5.1 Subject to Section 4, personal information, whether all or part of a client record, will not be released to third parties without the written consent of the client or the client's representative (e.g. their substitute decision maker, persons with power of attorney for personal care, legally appointed guardian or executor of an estate). Where a representative of a client is making a request for personal information, they must submit documentation verifying their legal standing as a representative of the client. A copy of this documentation will be kept in the client file.

5.2 Clients or their representatives are required to complete the FST *Consent for the Release of Information Form* or the *Consent for the Exchange of Information Form*, depending on the nature of the request. Consents provided on these forms are valid for 90 days from when authorization is given if it is for a one-time release of information or one year when a contracted or cooperating service provider requires the release of information for ongoing service provision, unless otherwise limited or withdrawn by the client in advance of that date. FST may disclose a client's personal information, provided that the disclosure, to the best of FST's knowledge, is for a lawful purpose.

5.3 Reports from third parties contained in a client record may not be released without the written consent of the third party. Clients will be encouraged to pursue access to this information directly with the third party.

5.4 In exceptional circumstances, where written consent is not possible, the oral consent of the client to the release of personal information will be accepted and will be recorded in the client's file.

5.5 In response to requests to release information to third parties, the FST service provider will determine if the reason to release information is valid, ensure that the client understands the purpose for which the information is being released and to whom the information is being released. The FST service provider will also explain that FST cannot guarantee the confidentiality of the information once it has been released.

5.6 Prior to the release of the file to the client, they will sign *FST's Consent form to release a file to client.*

5.7 FST may use individual data in aggregate form with no risk of personal identification of data for the development of public policy, statistical reporting to funders, the Board and to the public (annual report). Aggregated data may also be used for the purposes of program planning and analysis.

6. Safeguarding of Personal Information

6.1 Client information stored electronically is protected by password. Access to the FST electronic database is limited on a need-to-know basis for added security.

6.2 Client information collected in hard copy form is stored in locked cabinets accessible only by FST personnel providing service to the client, and the relevant program managers.

6.3 Access to client information will be limited to those who need to know the information for the purposes set out in the client's consent or as otherwise permitted or required by law or contract.

6.4 FST personnel will never leave client personal information, in paper or electronic form, unattended or exposed to anyone other than the client.

6.5 FST will not send confidential personal information to clients by email without the client's prior consent. Personal information sent to clients or about clients will employ password protected documents and/or secure email. If clients state they do not wish to receive emails in a secure method FST staff inform clients that FST does not accept responsibility for communications sent in a non-secure way. This is documented in the client's file.

6.6 Client information transmitted via email to third parties shall be sent in an encrypted format.

6.7 Communication between staff within the familyservicetoronto.org domain is secure in transmission. Client numbers and/or initials will be employed as a means of communication.

6.8 Web-based counselling will use an encrypted platform to protect client privacy and confidentiality.

6.9 In programs where funders require specific levels of security, documents will be clearly labelled as required by funders (for example, Protected A and Protected B for IRCC funding).

6.10 FST requires external agents, such as third-party auditors, to maintain the confidentiality of client information and to refrain from using client information for any purpose other than the purposes for which consent was provided by the client. Where appropriate and necessary, FST will obtain the consent of the client to disclosure of information to external agents. (External agents are persons or companies with which FST has contracts and that may come into contact with personal information.)

6.11 When disposal is permitted or required, records of client personal information will be disposed of in a secure manner such that reconstruction of the records is not reasonably foreseeable in the circumstances.

7. Notice to Clients of Theft, Loss, Unauthorized Access, Use or Disclosure of Client Information

7.1 Personnel are required to report to their supervisor and to the FST Privacy Officer (the Director of Changing Lives and Family Violence), any theft, loss, unauthorized access, use or disclosure of personal information of FST clients immediately upon becoming aware of this either verbally or via email. The Privacy Officer will follow up the report with FST's *Client Privacy and Confidentiality Incident Management Form or will solicit like information required on the form* within 24 hours of the initial report being made. In programs where funders require it, supervisors will file a serious occurrence report and respond to all queries from funders.

7.2 In the event of such theft, loss, unauthorized access, use or disclosure of personal information of an FST client, FST will immediately launch an investigation into the breech and notify the client as soon as possible.

7.3 Oral contact with the clients will be logged in the client record and will be followed up by a letter, which will be included in the client record.

7.4 In the case of former clients, contact will be made orally, if possible, and also in writing, at the last known address for the client recorded in FST's database.

7.5 The Chief Privacy Officer maintains a centralized registry of incidents and reports on these, in a non-identifying way, on a quarterly basis to the Board.

8. Client Access to and Correction of Personal Information

8.1 Clients wishing to review their records should contact the FST service provider, relevant program manager or Privacy Officer.

8.2 The request to view records can be made orally or in writing via email or letter. However, to engage in the formal access request under PHIPA (timeframes, right of complaint and appeal) the request must be made in writing.

8.2 Within 30 days of any such request, an appointment will be made for the client to review their personal information in a confidential manner on FST premises, in the presence of an FST employee, unless FST is entitled to refuse the request, in which case written notice will be given. Up to 60 days may be required in the case of complex searches (e.g., numerous records exist) where the time limit would unreasonably interfere with FST operations and/or a consultation is needed.

8.3 Clients may bring a support person to this appointment if they wish. Clients will show a copy of picture identification to verify their identity. When this is not possible, key identifying information based on client demographics recorded in the electronic client database will be requested from the client. In exceptional circumstances (e.g., a client is unable to come to the FST office due to health issues), a copy of the record may be sent by registered mail or secured by email to the individual with consent and verification of their identity. Where indicated, safety precautions related to the receipt of the file will be reviewed with the client and documented in the record prior to its release.

8.4 If a client representative is requesting to view the records on behalf of the client, documentation must be provided confirming the representative's identity and the relationship (either legal documents or signed consent by the client). Where FST receives signed consent from a client, FST will verify that the client understands what they have consented to.

8.5 FST is required to retain client personal information that is the subject of a request for access for as long as necessary to allow the client to exhaust any recourse under the *Personal Health Information Protection Act, 2004* that they may have with respect to the request. This may require FST to maintain the record for longer than the typical client record retention period detailed in the *Record Retention* policy.

8.6 Clients who wish an explanation of their records may contact their FST service provider, the relevant supervisor or the FST Privacy Officer.

8.7 Clients will not be permitted to access third party records without the consent of the third party. In such cases, the FST service provider will direct the client to obtain the requested information directly from the third party.

8.8 Clients wishing to correct information in their file shall provide the correction in writing to FST. The written correction will be included in the client's record and, within three weeks of receipt, FST will notify the client of its response to the correction.

8.9 In instances where clients request a copy of their record, they will be required to sign a form acknowledging that FST retains no responsibility for the record once it is released.

9. Exceptions to right of access by clients to their records

9.1 Refusing access to a client record can only be done in limited and specific situations including:

- the information in question is subject to a legal privilege (e.g.solicitor-client privilege or settlement privilege) that prohibits disclosure of
- could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual or serious bodily harm to the individual or another person.
- the information was collected in the course of an inspection, investigation or similar procedure and the resulting proceedings, appeals or processes have not yet been concluded.
- another law prohibits the disclosure of that information.

9.2 If it is believed that access to a record would likely cause serious harm to a client, personnel will consult with their manager and Director.

9.3 The Director will review the file, and if they are in agreement, will enter a note into the case record indicating the reason for refusal. The Privacy Officer may also be consulted.

9.4 An individual must still be provided with access to the part of the record that can reasonably be separated from the part of the record that the individual does not have a right of access to.

10. Appointment of Privacy Officer

10.1 The Privacy Officer for FST is the Director of Changing Lives and Family Violence. The Privacy Officer is responsible for all client-related inquiries and complaints.

10.2 The name and contact information for the Privacy Officer is available on the FST website, in the *Client Rights Statement* and in the FST Employees Directory.

10.3 The duties of the Privacy Officer include:

- maintaining knowledge of privacy legislation and regulations
- ensuring that all employees and volunteers have training on the privacy policy

- monitoring employee compliance with FST's privacy policy
- responding to privacy-related complaints and concerns
- responding to requests for access and correction
- responding to inquiries from the public about FST's privacy practices
- liaising with other organizations, the public and government, as necessary, on privacy-related issues.

11. Inquiries and Complaints

11.1 Questions, comments or complaints about the FST privacy policies and procedures or about the collection, use or disclosure of personal information will be directed to the Privacy Officer.

11.2 The Privacy Officer will follow the procedures set out in the *Service User and Community Member Complaints* policy in responding to, resolving and recording privacy-related complaints.

11.3 If the client is not satisfied with the response provided by the Privacy Officer, the client may contact the Office of the Information and Privacy Commissioner of Ontario, in writing, at 2 Bloor Street East, Toronto, Ontario, M4W 1A8 or by calling 416-326-3333.

12. Confidentiality and Privacy Agreement

12.1 All FST personnel will sign a Confidentiality and Privacy Agreement as part of their initial hiring or orientation. The signed Agreement will be placed in their file. Personnel will not have access to any confidential information until after they have signed the Agreement (e.g., will not provide service to clients, access client or personnel records).

12.2 Any breach of confidentiality whether real or suspected should be reported as follows:

- if related to clients and donors, the breach should be reported to the relevant supervisor who will involve the FST Privacy Officer
- if related to personnel, the breach should be reported to the relevant supervisor who will involve the Director of Human Resources
- if related to financial matters, the breach should be reported to the relevant supervisor who will involve the Director of Finance.

CONSENT FOR RECORDING, PHOTOGRAPHING AND/OR FILMING

Personnel as well as all clients and members of the public will be asked to provide their informed and/or written consent prior to any recording, photographing or filming that may be used for promotional, educational or training purposes by the organization. Requests for participation in media-conducted interviews or other activities for publication in print, online and/or for broadcasting purposes will be co-ordinated through Technology and Communications with specific waivers provided by the media organization.

FST PROPERTY

Upon termination of employment or placement with FST, personnel shall promptly return (without duplicating or summarizing), any and all material pertaining to FST business in their possession including, but not limited to: all client information (charts, lists, etc.), physical property, documents, keys, electronic information storage media, manuals, letters, notes and reports.

LEGAL

This agreement will not supersede any legal obligation to disseminate information when required to do so in a court of law or contract.

Updated Nov. 17, 2021