

Policy Name and Number:	1.11 Confidentiality and Privacy
Source:	Best practice, legislation
Date Last Reviewed:	November 17, 2021
Approval or Last Revision:	May 21, 2025
Approved By:	Board of Directors

POLICY

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

The following is considered confidential information however; some categories are classified as “Restricted” under policy 11.10 Data Classification and require higher levels of protection:

- All matters/documentation relating to clients (restricted)
- All contracts.
- All Human Resources files and proceedings.
- All financial and banking information, status and statements (restricted)
- 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 personnel (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.

Aggregated data will be utilized with no risk of personal identification for public policy development, service evaluation, internal statistical reporting, program planning, and reporting to funders, the Board, and the public.

SCOPE

This policy applies to all FST personnel (employees, students, volunteers) and board members and unless specified, to both confidential and restricted data.

REQUIREMENT OF CONFIDENTIALITY

In accordance with PHIPA (Personal Health Information Act), FST requires all personnel to handle sensitive personal client information in a confidential and appropriate manner. It is understood that FST personnel will become aware of confidential information regarding our clients through the course of their employment. Personnel 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. Personnel 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
- 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 are able to 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 in order 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 personnel, FST personnel 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, and the original copy consent will be destroyed. A note will be made in the client's record that the form has been signed.
 - 1.5 In cases where it is not possible or practical to obtain the client's written acknowledgment (e.g., telephone only service), 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 of the individual must be knowledgeable, relate to 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 personnel are concerned that a client does not have the capacity to consent to the collection, use and disclosure of their personal

information, personnel 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, personnel will implement the following "lock-box" procedure.
- 2.3 Electronic records stored in TREAT: FST personnel 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.
 - Scan any written instructions by the client into the client's electronic record.
 - Activate the alert button on the person/client page for the client in the FST electronic database, thus notifying employees accessing the file of the withholding, limiting or withdrawal of consent.
 - Notify the Privacy Officer or their designate of the client's instructions. The Privacy Officer will reach out to the client to review their request and discuss various options available, including the activation of a lock-box and/or other means of further securing their record (e.g. name change, address change)
 - Upon receiving instructions from the client, and where a client opts for a lock-box, the Privacy Officer will lock the file electronically.
 - The level of access to the file will be determined with the client (e.g. lock out one or more staff known to the client; lock out all staff except the staff person providing support, subject to provisions below)
 - The staff person providing service to the client, the staff person's manager, in the case of a student the field instructor, the Privacy Office and the Operations Manager will be added to all lock boxes. This will be done so the manager/field instructor can provide adequate supervision and the Operations Manager can facilitate any additional intake requests from the client. The Privacy Officer is named since they have the rights to add lock boxes.
- 2.4 In situations where the withholding, limiting or withdrawal of consent will limit or prevent FST from continuing to deliver services, personnel 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 an FST funder; former FST 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 A list of the aliases, clients' real names and file numbers will be confidentially 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 must be informed of these limitations on confidentiality.
- 3.5 Human Resources 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 the past, an alias will be assigned to the record in order to maintain the privacy of the new FST personnel.

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* or an arbitrator) or
 - It is otherwise permitted or required by law.
- 4.2 If FST personnel are served with a warrant, summons, subpoena, 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. A request to access legal counsel will be made to the Chief Operating Officer by the Privacy Officer.

- 4.3 In general, where an order, summons, warrant, subpoena 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".
- 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. In instances where FST is legally compelled not to notify the client, the organization will comply, and a note will be made in the client's file.

5. **Release of Information to Third Parties with Client Consent**

- 5.1 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 substitute decision maker, where applicable. Clients 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. Consent 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.
- 5.2 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. 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.
- 5.3 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.

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 Random log audits of TREAT records are generated by FST's Business

Intelligence team on a quarterly basis and managers are required to review the activity of any of their staff audited with the purpose of determining if their access to the client record is valid.

- 6.3 Client information collected in hard copy (e.g. in the event an electronic client database goes offline) must be made in a way that does not identify the client (e.g. by client number), stored in a locked space accessible only by FST personnel or on FST's secure network. All notes must be transferred into the client's file no later than 48 hours after being collected unless there are exceptional circumstances (e.g. an electronic client database is not available) and securely destroyed.
- 6.4 Access to client information is 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.
- 6.5 FST personnel will never leave client personal information, in paper or electronic form, unattended or exposed to anyone other than the client.
- 6.6 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 secure email (Note that secure email ensures messages are encrypted). If clients state that they do not wish to receive emails in a secure method FST personnel inform clients that FST does not accept responsibility for communications sent in a non-secure way. This is documented in the client's file.
- 6.7 Client information transmitted via email to third parties shall be sent in an encrypted/password protected format.
- 6.8 Communication between personnel within the familyservicetoronto.org domain is secure in transmission. Client numbers and/or initials will be employed as a means of communication and all emails are marked confidential within the subject line.
- 6.9 Web-based counselling will use an encrypted website to protect client privacy and confidentiality.
- 6.10 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 CIC funding).
- 6.11 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.)
- 6.12 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, Clinical Services), 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. This communication will be followed up by completion of the Client Privacy and Confidentiality Incident Management Form within 24 hours of the initial report being made. In programs where funders require it, supervisors will file a serious occurrence report in this situation.

- 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 breach 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, should the client indicate, they would like to receive a letter when asked, 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 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 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 a 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 for records. Clients may bring a support person to this appointment if they wish. Clients will show a copy of picture identification to verify their identity. 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 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.
- 8.3 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 he or she 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.
- 8.4 Clients who wish an explanation of their records may contact their FST service provider, the relevant supervisor or the FST Privacy Officer.
- 8.5 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.
- 8.6 Clients wishing to correct information in their file shall provide the correction in writing to FST. FST will review all correction requests and will involve the

writer(s) of the record where indicated and feasible (e.g. writer of record). 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.

- 8.7 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. Appointment of Privacy Officer

9.1 The Privacy Officer for FST is the Director, Clinical Services. The Privacy Officer is responsible for all client-related inquiries and complaints.

9.2 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.

9.3 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.

10. Inquiries and Complaints

10.1 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.

10.2 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.

10.3 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.

11. Confidentiality and Privacy Agreement

11.1 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 personnel 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).

11.2 Any breach of confidentiality whether real or suspected shall be reported as follows:

- if related to clients and donors, the breach will be reported to the relevant supervisor who will involve the FST Privacy Officer

- if related to personnel, the breach will be reported to the relevant supervisor who will involve the Senior Director, People and Culture.
- if related to financial matters, the breach will 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 coordinated through the Communications department with specific waivers provided by the media organization.

FST Property

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

Upon leaving the organization, an individual's user account is deactivated on their last day of employment, volunteer or student placement.

Legal

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

Additional Reference

11.10 Data Classification



FAMILY SERVICE TORONTO

For People. For Change.

CONFIDENTIALITY and PRIVACY AGREEMENT

I, _____, acknowledge that I have read and understand the Confidentiality and Privacy policy of Family Service Toronto. I agree to adhere to this policy in its entirety and, where applicable, I will ensure that employees, students and volunteers working under my direction adhere to this policy.

I agree to maintain confidentiality regarding the confidential business activities, processes, and practices of FST and all information related to our clients, former clients and community participants at all times during and after my involvement with Family Service Toronto as an employee, student or volunteer. Furthermore, I understand that if I violate the rules set forth in the Agreement, I may face disciplinary action up to and including termination and/or legal action as necessary.

Name:

Signature:

Date:

Witness:

Original to: Human Resources for placement in HR file