Saint Dominic's Family Services

Client Information Privacy and Confidentiality Policy

POLICY NUMBER	EFFECTIVE DATE	LAST REVISED	APPLICABLE TO
ENT-POL-302-01	11/04/2026	NA	Enterprise

I. Purpose

To establish requirements for the collection, use, disclosure, and protection of client information to safeguard confidentiality, prevent unauthorized access or disclosure, and ensure compliance with applicable privacy requirements.

II. Scope

This policy applies to all SDFS employees and authorized third parties who collect, access, use, maintain, or disclose client information. It covers all client information maintained or processed by SDFS or authorized third parties, regardless of format or location.

III. Definitions

Personally Identifiable Information (PII)
Information that can identify an individual, either on its own or when combined with other information.

Opt-Out Notice
A notification informing individuals of their right to decline certain sharing of their personal information with third parties.

Sensitive Personal Information
Personal information requiring additional protection due to its confidential nature, including medical, financial, or other information classified as sensitive by SDFS.

Third-Party
An individual or organization outside SDFS that is authorized to receive, access, or process personal information.

IV. Policy

A. Privacy Notices and Client Rights

SDFS shall maintain written privacy policies describing how sensitive client information is protected. Privacy policies relevant to current and prospective clients shall be publicly posted and distributed, at least annually, along with instructions for opting out of data sharing activities, where applicable.

When material changes are made to these policies, SDFS staff shall promptly notify the affected clients and highlight the key changes when distributing the updated policies.

Upon receiving a verified request from a client, SDFS shall provide the following information regarding its collection and use of the client's personal information:

- The categories of personal information collected about the client;
- The categories of sources from which the information was collected;
- The business or operational purposes for collecting or selling the information;
- The categories of third parties with whom the information is shared; and
- The specific personal information collected about the client.

If SDFS is unable to provide the requested information, the client shall be promptly notified of the reason for the denial.

B. Collection and Use of Personal Information

SDFS shall collect private information only through lawful means and for purposes related to agency operations. The collection, processing, storage, and disclosure of private information shall be limited to what is necessary for agency operations. Personal information shall only be used for the purposes disclosed at the time of collection, and any new or additional uses shall require the individual's approval.

Before collecting personal information, SDFS shall provide current and prospective clients, as applicable, with its Notice of Privacy Practices and an opportunity to review the notice and ask questions. SDFS shall obtain informed consent prior to collecting personal information and written consent before entering such information into an SDFS computerized information system.

1. Revocation of Consent

When an individual revokes previously granted consent for SDFS to use their personal information, SDFS shall promptly update its records and ensure the individual's decision is honored.

2. Consent for Provision of Services

Before services are provided, SDFS shall obtain written consent from clients authorizing the disclosure of their personal information to SDFS staff and authorized third parties who require access to provide those services.

The Chief Program Officer (CPO) or designee may waive this requirement in an emergency or when substantial communication barriers prevent the client from providing written consent.

At the time information is collected, SDFS shall provide clients and prospective clients with:

- A clear and accurate description of the information being collected and how it will be used;

- An explanation of the consequences, if any, of refusing to provide the requested information; and
- SDFS's legal name and current contact information, unless this information is readily available elsewhere on the user's screen.

Notice of the collection of personally identifiable information (PII) shall be provided at the time and place of collection. Information regarding the collection of non-personally identifiable information shall be included in SDFS's publicly posted privacy policy.

SDFS shall not collect biometric information through its information systems without first notifying the individual and obtaining their consent.

3. Collection of Children's Personal Information

SDFS shall not collect children's personal information through its information systems without first obtaining informed consent from the child's parent or guardian.

4. Use of Location Information

SDFS shall not use location information obtained through electronic devices to identify the location of clients or employees for marketing purposes, or permit third parties to use such information for marketing, without the individual's specific authorization.

C. Consent to Receive Text Messages

Clients and/or their support networks are not required to consent to receiving text messages from SDFS.

By providing their phone number and opting in, they consent to receive text messages from SDFS regarding inquiries, SDFS services, or related legal matters. Message and data rates may apply. Clients and their support networks can opt out of receiving text messages at any time by replying "STOP" to any text message they receive from SDFS. Opting out may limit SDFS' ability to communicate with clients and their support networks regarding their case or services. See "SMS Terms and Conditions" (attachment A) for more details.

1. Information Sharing and Disclosure

No mobile information will be shared with third parties/affiliates for marketing/promotional purposes.

SDFS will not sell or rent clients and/or their support networks' personal information to third parties. SDFS will not sell, rent, release, or transfer clients' and/or their support networks' SMS consent or phone number to any third party for any third-party marketing purposes.

SDFS may share clients and/or their support networks' information in the following circumstances:

2. Service Providers

SDFS may share clients' and/or their support networks' information with its service providers who perform services on the agency's behalf. These service providers must be contractually obligated to protect the clients' and/or their support networks' information and use it only for services they provide.

3. Legal Requirements

SDFS may disclose clients' and/or their support networks' information if required by law, regulation, or legal process.

4. Data Security

SDFS must implement reasonable security measures to protect clients' and/or their support networks' personal information from unauthorized access, use, disclosure, alteration, or destruction. However, no method of transmission over the internet or electronic storage is completely secure, and SDFS cannot guarantee absolute security.

D. Accuracy and Correction of Client Information

SDFS shall provide clients with access to their personal information and a process to request corrections, deletion, or restrictions on disclosure to third parties when information is believed to be inaccurate or outdated.

Upon receiving notice that personal information is inaccurate, SDFS shall promptly correct the information or document in the record that its accuracy is disputed.

1. Change of Contact Information

Client requests to change a mailing address shall take effect one month after the change is entered into the system. Requests to change an email address shall take effect two business days after entry. SDFS shall confirm both types of changes by sending a notice to the client's previous address.

E. Disclosure and Transfer of Personal Information

SDFS staff shall document all disclosures of personal information to third parties, including the information disclosed, the recipient, and the date of disclosure. These records shall be retained for at least five years.

1. Third-Party Disclosure Requirements

SDFS shall disclose or transfer sensitive personal information to third parties only when the individual has been notified of and provided affirmative consent (opted in) to the disclosure or transfer. Non-sensitive personal information may be shared in accordance with SDFS's privacy policy unless the individual has opted out.

Third parties receiving personal information must agree to comply with the privacy policy in effect when the information was originally collected.

Exceptions may be made when:

- Disclosure or transfer is required by a court order or other governmental directive;
- The individual submits a written request authorizing the transfer; or
- The individual agrees to a new privacy policy permitting the transfer.

Third-party organizations receiving personal information must also provide a written commitment to maintain an adequate level of protection, as determined by the Chief Executive Officer or designee, unless disclosure is required by law or regulation.

2. Transfers Following Organizational Changes

In the event SDFS is sold, merged, acquired, ceases operations, or otherwise undergoes an organizational change, personal information may be transferred to another entity as necessary to continue providing services. Affected clients shall be promptly notified of the transfer.

Personal information transferred under these circumstances shall not be used for new or previously undisclosed purposes without the individual's affirmative consent (opt-in).

3. Third-Party Custodians

Personal information transferred to a third-party custodian shall be provided only to an identified custodian who agrees to maintain current records of all individuals subsequently granted access to the information, including their names, addresses, and organizational affiliations.

F. Information Security and Access Controls

Access to personal information maintained by SDFS shall be restricted to authorized staff on a need-to-know basis and used only for legitimate agency purposes.

Staff shall maintain the confidentiality of client identities and shall not publicly identify or discuss clients, including individuals who may be publicly known, except when necessary to perform authorized agency duties. Any necessary disclosure shall be handled discreetly and professionally.

1. Access Monitoring and Logging

SDFS shall restrict access to systems containing private information and maintain a log of each access, including whose information was accessed, who accessed it, and the date and time.

2. Protection of Personal Identifiers

SDFS information systems shall not use hidden serial numbers, personal identification numbers, or other undisclosed mechanisms that could reveal a client's identity or activities.

Personal identifiers, including Social Security numbers, shall not be displayed in publicly accessible locations or materials controlled by SDFS, including websites, publications, and

other public communications. Public encryption keys and digital certificates are exempt from this restriction.

Social Security numbers and other personal identifiers that are not necessary for the recipient shall not be included in client statements or communications, whether transmitted electronically, by mail, or through other methods.

SDFS shall not use Social Security numbers, driver's license numbers, or other externally identifiable personal information as internal client account numbers.

3. Examination of Private User Files

Authorized systems administrators may examine private user files when necessary to address emergencies, security concerns, system maintenance, or other legitimate operational needs, including virus removal and backup restoration.

Affected users shall be promptly notified when their files are examined, unless an investigation of alleged abusive or criminal activity is underway. Any copies created during the examination shall be securely destroyed once the matter has been resolved, in accordance with applicable SDFS records retention and destruction requirements.

4. De-Identification of Personal Information

Personal information no longer required for legal, regulatory, or operational purposes shall be promptly de-identified so that the information retained can no longer be linked to the individuals involved.

V. Violations of this Policy

Any violation of this policy may result in disciplinary action, up to and including termination of employment. SDFS reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. SDFS does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, SDFS reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

References

- CPL: 16.2 Customer Privacy Management
- ISO 27002: 18.1.4 Privacy and protection of personally identifiable information
- HIPAA Privacy Rules
- NIST: Appendix J Privacy Controls (800-53 V5 P Controls)

- US-CSF: PR.DS-9 Privacy of individuals and (PII) is protected
- SDFS Information Classification Policy
- SDFS Data Breach Response Policy

Saint Dominic's Family Services

SMS Terms and Conditions

Attachment A to Client Information Privacy & Confidentiality Policy (ENT-POL-302-01)

These Short Message Service (SMS) Terms & Conditions outline the text message practices of Saint Dominic's Family Services (SDFS), including consent, fees, and opt-out options.

1. SMS Consent and Privacy

The phone numbers obtained as part of the SMS consent process will not be shared with third parties for marketing purposes.

2. Types of SMS Communications

If you have consented to receive text messages from SDFS, you may receive messages related to the following:

- Reminders
- Follow-up messages
- Billing inquiries
- Announcements
- Agency or service updates
- Surveys

Example: "Hello, this is a friendly reminder to complete your survey. Reply STOP to opt out of SMS messaging at any time."

3. Message Frequency

Message frequency may vary depending on the type of communication. For example, you may receive up to one (1) SMS message per week related to your satisfaction survey.

4. Potential Fees for SMS Messaging

Please note that standard message and data rates may apply, depending on your carrier's pricing plan. These fees may vary if the message is sent domestically or internationally.

5. Opt-In Method

You may opt-in to receive SMS messages from SDFS either verbally or in writing.

6. Opt-Out Method

You can opt out of receiving SMS messages at any time. To do so, simply reply "STOP" to any SMS message you receive. Alternatively, you can contact SDFS directly to request removal from the agency's messaging list.

7. Help

If you are experiencing any issues, you can reply with the keyword "HELP."

8. Standard Messaging Disclosures

- Message and data rates may apply.
- You can opt-out at any time by texting "STOP."
- For assistance, text "HELP" or visit our Client Information and Confidentiality Policy and/or SDFS' Terms and Conditions pages found on our company website.
- Message frequency may vary.