St. John Ambulance Saint-Jean

PRIVACY POLICY

Policy Objective	The purpose of this policy is to protect the personal information of all of St. John Ambulance's internal and external stakeholders, and to comply with applicable legislation.
Policy Statement	St. John Ambulance is committed to protecting any and all personal information that it collects on its members, staff, and clients. This policy is intended to ensure that its protection of personal information complies with all applicable provincial/territorial/federal legislations.
Effective Date	January 2004
Applies To	All personnel affiliated with St. John Ambulance in any capacity (paid or unpaid). The Privacy Policy applies to all third party providers, which includes general public instructors who receive personal information for processing. The Privacy Policy applies to all St. John Ambulance policies. Privacy guidelines respecting Community Services shall be contained within the policies and/or procedures for each governance and operational area contained within the NOPP Manual.

Policy Context

St. John Ambulance (SJA) respects an individual's privacy. We protect personal information and adhere to all legislative requirements respecting an individual's privacy. We do not rent, sell or trade our mailing lists. The information provided to us will be used to deliver our services and to keep the individual informed and up to date on SJA's programs, services and activities. The SJA Privacy Policy is designed to ensure compliance with federal privacy legislation.

Privacy Principles

1. *Accountability*
   SJA is responsible for the protection of all personal information under its control.

2. *Identifying Purposes*
   SJA must document why it is collecting the information before it is collected and advise an individual of new and/or additional purpose for collecting personal information and seek consent unless otherwise required or permitted by law.

3. *Consent*
   The individual must consent to the collection, use or disclosure of the information except where required or permitted by applicable law.

4. *Limiting Collection*
   The information collected on the individual must be limited to information for the purpose identified by SJA.

5. *Limiting Use, Disclosure, and Retention*
   Personal information can only be used or disclosed for the purpose for which it was collected unless the individual has consented or as required or permitted by law.

6. *Accuracy*
   Personal information must be maintained as accurate and complete as is necessary for the purpose for which it was to be used.

7. *Safeguards*
   SJA must protect personal information against loss, theft and safeguard information from unauthorized access by implementing security safeguards appropriate to the sensitivity of the information regardless of the format in which it is held.

8. *Openness*
   SJA has an obligation to make public its personal information protection policies and practices.

9. *Individual Access*
   SJA has an obligation to grant an individual access to the personal information that has been collected about them.

10. *Challenging Compliance*
    Individuals may direct questions and inquiries with respect to the ten principles outlined above or about our practices by contacting the respective Council within their jurisdiction or the Privacy Officer at National Office of SJA.

Definitions

Note: The SJA Privacy Policy is often distributed independently of the NOPP-CS Manual. Therefore, a number of standard SJA terms (e.g. Council, jurisdiction) have been defined here to ensure clarity.

Clients – recipients of training courses, products and/or community service programs (paid or unpaid) and donors.

Council – SJA operations within each province and/or territory and is controlled by SJA Provincial/Territorial Office (a separately incorporated charity) that is known as St. John Council for *Province/Territory e.g. St. John Council for Ontario.*

Historical records – records that are retained on a permanent basis and include

- constitution and by-laws,
- committee, Board of Directors and Annual General Meeting minutes,
- selective retention of building and site contracts, land titles, environmental studies on properties,
- records relating copyright or trademark applications,
- selective retention of financial audits for archival purposes,
- funds – bursaries and scholarships,
- records relating to legal issues, opinions and advice provided to the Board of Directors,
- selective retention of public relations records– newspaper clippings, media relations documents (e.g. press releases),
- risk management records and insurance records,
- donor records,
- member service records,
- community service volunteer admission and promotions in the Order of St. John, and
- commemorative medal recipients.

Jurisdiction – refers to the SJA Councils and their respective operating centres (branches), and any community service divisions, units, fellowships, instructors that may be within their respective.

Members – Members of the Order, Board Members, volunteers, instructors, and staff.

Order of St. John – The Most Venerable Order of the Hospital of St. John of Jerusalem (Order of St. John) is an international charitable humanitarian organization, active in Canada for more than 118 years. SJA is one of two foundations of the Order of St. John.

Personal information – is any personal identifiable information that is not the name, title, business address or contact information of an employee of an organization. Personal information about an identifiable individual may be factual or subjective, recorded or not. Personal information refers to or includes:

- all personal information that is collected, used or disclosed within the control of SJA as an organization operating across Canada
- information that is collected, used or disclosed by SJA at all levels of the organization including National Office (federally incorporated charity) and Provincial/Territorial Councils (separately incorporated charities) and their respective Branch(s), Divisions and Unit levels.
- information provided by members (Members of the Most Venerable Order of the Hospital of St. John of Jerusalem (the ”Order”), volunteers, instructors, staff, and clients.
- information in all formats including paper-based and electronic and in all locations.

PIPEDA – Personal Information Protection and Electronic Documents Act

Priory Council – The Board of Directors of the Priory of Canada whose trade name is SJA.

Record – any correspondence, memorandum, report, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, documentary material.

Third party providers — a third party is a company or organization that has been contracted by SJA to provide services. The third party provider may have direct access to personal information. Examples of third party providers may include Management of IT services, mailing house for the distribution of bulk mail, consultants required to develop and/or support a database containing personal information, and the like. However it does not include key internal business functions such as payroll functions.

Policy Requirements

1. Identifying purposes—SJA must document and inform individuals why it is collecting the information before it is collected and advise an individual of new and/or additional purposes for collecting personal information.

1.1 A purpose and use statement is required for all personal information collected by St. John Ambulance. A purpose and use statement must be included on any form used for collecting personal information.
1.2 Each description of the purpose for collection of personal information must be accurate and easy to understand.

2. Consent—The individual must consent to the collection, use or disclosure of the information except where required or permitted by applicable law.
   2.1 For all collections of personal information (regardless of which collection tool is used) SJA is required to ensure consent has been obtained for the identified purpose and/or use of the required personal information and advise the individual of consequences should consent not be obtained.
   2.2 If consent is not obtained, the personal information will not be collected or used for the respective purpose.
   2.3 "Grandfathering" of consent is not permitted. For example, if past practices have included collecting information on individuals' hobbies, such a practice is no longer allowed without receiving consent to collect such information. Members and clients must be notified in writing of the SJA Privacy Policy, the current types of personal information that has and is being collected and the respective use of this information.
   2.4 Implied consent may be deemed to have been received in the following circumstances.
      - The personal information was collected, used and/or disclosed to provide a product, program and/or service.
      - The personal information was collected, used and/or disclosed while the individual held a position within SJA.
      - The personal information was collected, used and/or disclosed for the purpose of providing someone with an honour or award.

   If implied consent has been received according to any of these circumstances, SJA must therefore limit the collection, use and disclosure of the personal information to the specified purpose.
   2.5 Existing staff and volunteers will be required to review the SJA Privacy Policy and sign a Statement of Compliance Form (see Attachment A of this policy).
   2.6 Should the purpose for collecting the personal information change, consent must be obtained for the new purpose.

2.7 SJA will not disclose personal information about any individual without their prior consent unless required or as permitted by law.

3. Collecting Personal Information—information collected on an individual must be limited to information for the purpose identified by SJA.
   3.1 Limiting collection—SJA will make every effort to ensure that personal information is not collected from individuals who are thirteen years (13) of age and under unless there is proof of parental consent. At its discretion, SJA will put in place restrictions to the collection, use and disclosure of personal information to limit any potential exposure of a child.
   3.2 Tools for collection—SJA uses a variety of tools to collect the information for the required purpose. These collection tools include but are not limited to, Customer Relationship Management software systems (UNITY), registration forms (for training courses, volunteer and/or events), email requests and/or submissions, web forms, fax forms, resumes, references, information provided by telephone call-ins and/or call-outs. The SJA Privacy Policy applies regardless of the collection tool used.
      - Each collection tool must have a brief description of the purpose, use and disclosure of personal information on the SJA Privacy Policy
      - Each collection tool must have a means of withdrawing consent or updating contact information.
      - Each collection tool shall include a consent question for the collection, use and/or disclosure of personal information for a secondary purpose.
      - Each collection tool must be completed up to the stage whereby the purpose of collection has been obtained to ensure that no additional collection is carried out without consent.

4. Limiting Use, Disclosure, and Retention—Personal information can only be used or disclosed for the purpose for which it was collected unless the individual has consented or as is required or permitted by law.
   4.1 Retention Schedules—a standard retention schedule for all records, drawn up in accordance with other SJA policies, is a minimum requirement and must be implemented by all jurisdictions, as outlined in the Records Management Policy (see Attachment B of this policy for the SJA Retention Schedule).

5. Accuracy—Personal information must be maintained as accurately and completely as is necessary for the purpose for which it was collected.

5.1 Individuals have the right to ensure the information within their file is accurate, complete and unambiguous. Any personal information may be deleted and/or removed should the record be out of date, or if it does not meet the purpose and/or use for which it was intended, with the exception of information required to maintain historical records and accurate statistics.

6. Safeguards—SJA must protect personal information against loss, theft and unauthorized access by implementing security safeguards appropriate to the sensitivity of the information regardless of the format in which it is held.
   6.1 SJA shall not sell, rent or trade mailing lists.
   6.2 Computer and Internet Security—a standard guideline for computer and Internet security is a minimum requirement and must be implemented by all jurisdictions as contained within the Information Technology Services Policy
   6.3 All individuals must be authorized prior to receiving access to databases containing personal information
   6.4 Staff Training—all employees and volunteers in supervisory positions must receive information and/or training on how to collect and safeguard personal information in compliance with the SJA Privacy Policy.

7. Individual Rights and Access to Personal Information—SJA is required to grant individuals access to the personal information that has been collected about them. Each member and/or client has the right to:
   - know why SJA collects, uses or discloses his/her personal information
   - know that SJA is protecting his/her personal information and that appropriate security measures are in place
   - ensure that his/her personal information is accurate, complete and up-to-date
   - obtain access to personal information and request any corrections as may be required
   - provide feedback about how an organization handles their personal information.

   7.1 Access to personal information located on the national database and/or at the national office, council or branch locations is granted by the national and provincial CEOs to the respective individual required to process the information for the delivery of programs, products and services. See the Procedures section of this policy for details on how to access personal information.

8. Compliance—SJA is required to ensure that its operations and practices comply with federal and provincial/territorial privacy legislation and its own organizational Privacy Policy.

8.1 National coordination—a National Privacy Compliance Team shall be comprised of one member identified by each of SJA's Provincial/Territorial Councils. Each compliance team member shall be known as the Privacy Officer for their jurisdiction and will be directly responsible for ensuring their respective jurisdiction adheres to the SJA Privacy Policy. The National Privacy Compliance Team shall have access to legal counsel as required.

8.2 Provincial/Territorial privacy legislation—each Provincial/Territorial Council is required to ensure that it complies with the specific requirements of its provincial/territorial privacy legislation. The Privacy Officer of each Provincial/Territorial Council will attach to this policy the specific privacy requirements in their provincial/territorial jurisdiction.

8.3 Complaints—to ensure proper and ongoing implementation of the SJA Privacy Policy, each Privacy Officer is required to report to the National Privacy Compliance Team any complaints and/or issues raised by an individual and/or organization. The Privacy Officer must maintain a log complaints for their respective jurisdiction(See the Procedures Section of this Policy for a description of the complaint process).

8.4 New products/programs—employees, members and volunteers who are developing new products and/or programs are required to consult with their local Privacy Officer to ensure that any new product and/or program meets SJA Privacy Policy requirements.

8.5 Third Party Non-Disclosure and Compliance Agreements—At a minimum, third Parties must sign an agreement that they will not disclose any personal information gathered or provided to them to perform and/or provide services for SJA. A sample confidentiality and non disclosure policy is available on the SJA Intranet site in The Privacy Toolkit section.

8.6 Audit—a committee will be identified within each Council and at the National Office to audit the implementation of the policy. The committee will be comprised of a minimum of two (2) members who shall be appointed by the CEO of the respective jurisdiction.

- Each Audit Committee is required to complete an annual privacy audit of its local operations to ensure compliance with this policy.
- Each Audit Committee is required to submit a compliance statement to Priory Council. These compliance statements must accompany and/or be included in annual reports distributed by Councils.
- Each Audit Committee is required to submit annual findings and recommendations to the National Privacy Compliance Team to include within the SJA Privacy Policy review.

- Individuals may direct questions and inquiries about SJA's Privacy Policy and it related practices by contacting the Provincial/Territorial Privacy Officer within their jurisdiction or the Privacy Officer at National Office of SJA**.**

Responsibility/Accountability

SJA is responsible for the protection of all personal information under its control.

1. The National Privacy Compliance Team is responsible for developing SJA Privacy Policy, including amendments and/or updates.

2. The National Office Privacy Officer is responsible for coordinating policy development and implementing the policy throughout the organization.

3. The National Management Team is responsible for approving the SJA Privacy Policy, its amendments and/or updates.

4. Provincial/Territorial Councils are required to monitor the application of the SJA Privacy Policy within their jurisdiction to ensure their compliance with the SJA Privacy Policy.

5. Provincial/Territorial Privacy Officers are responsible for:
   - ensuring that the SJA Provincial/Territorial organization adheres to provincial/territorial privacy legislation;
   - ensuring that particular concerns about provincial/territorial privacy legislation requirements are brought to the National Compliance Team for consideration;
   - ensuring that changes or amendments to provincial/territorial privacy legislation are noted and complied with.
   - The Privacy Officer must maintain a log of complaints at the respective jurisdiction.

6. Local SJA Branches and Offices, and all personnel (paid and unpaid) affiliated with SJA and involved in collecting personal information are responsible for adhering to this SJA Privacy Policy.

Procedures

Procedures for implementing the SJA Privacy Policy are as follows:

- ensure that information regarding the SJA Privacy Policy is available to members, clients and event sponsors. Standard information forms are available on the SJA Intranet.
- ensure that when collecting personal information, either over the phone, electronically and/or using collection tools such as forms, through a website form and the like, that members are provided with the information as per section 1.0. and consent is received. Where possible, records of consent are retained for the period of time in which the information is to be used.
- provide training and information on the SJA Privacy Policy to all employees, instructors and volunteers.
- review all operational policies to ensure compliance with privacy-related procedures

Clients of SJA Community Services Programs

As a representative of SJA, instructors, volunteers, and employees have an obligation to ensure that our clients are aware of SJA's Privacy Statement as it relates to the delivery of services.

New Employees, Instructors, and Board Members

- All new members must receive a copy of the SJA Privacy Policy and receive training from a designated individual trained on the SJA Privacy Policy within SJA.
- Each new member is required to sign off on the SJA Privacy Policy (See Privacy Compliance Form on page 15 of this policy - Privacy Compliance Form) as having understood their obligations under the policy.
- Members are only permitted to have access to personal information as required to carry out their responsibilities as outlined within their respective position descriptions.

Requests for Information on an Individual by a Third Party

To provide a third party with personal information about an individual, consent must be received from the respective individual.

Requests for Access to Personal Information

1. An individual must submit a written request to the Branch or Council operating in their province/territory to access his/her personal information being held by SJA.

2. Following the acknowledgement of receipt of the request, the Branch Manager or CEO and/or designate will respond to the request within 30 days from receipt of the request, or such other time period as applicable by law.

3. Exceptions to providing access to personal information include:
   - requests for to access nomination information for admission or promotion in the Order specifically, SJA will not provide access to personal information before nominations have been approved, but will provide access to information after nominations have been approved.
   - conflict with another individuals right to privacy, unless consent is received, i.e. divulging complainant's name.

Complaint Process

Submitting a complaint

1. Complainants must submit a written complaint to the CEO of the related jurisdiction.
2. The CEO will forward the written complaint to the Privacy Officer.
3. The Privacy Officer will acknowledge the complaint by giving a letter of receipt to the complainant within 30 days receipt of the written complaint.
4. The Privacy Officer will enter the complaint in the complaint log and notify the SJA National Privacy Officer of the complaint.

Investigating the Complaint

1. The Privacy Officer will appraise the complaint and determine the issues and/or validity of the complaint.

2. The Privacy Officer will write a letter to the complainant stating that the complaint has been received and that the complainant will be advised within 30 days whether the complaint is accepted or rejected.

3. If the complaint is rejected, the Privacy Officer will send a letter to the complainant stating the complaint has been rejected and including the rationale for the rejection. The letter will state that SJA now considers the matter to be closed. The complainant may appeal the decision if there has been an error in the review process.

4. If the Privacy Officer validates the complaint, a formal assessment will be undertaken and the complainant will be advised in writing that an investigation will be conducted. SJA will try to complete the complaint investigation process within 30 days following the initial assessment of validity.
   4.1 The local CEO will decide the appropriate approach for investigating the complaint. A fact finding exercise may include establishing an investigation team consisting of the Privacy Officer and a minimum of 2 other members. The nature and scope of the complaint will determine the need for an investigation team. The investigation team will report their findings to the CEO.

4.2 The investigation team may use a variety of approaches to try to resolve the complaint. Acceptable approaches include:
- interviewing the complainant;
- creating a dispute resolution process;
- requesting that a privacy audit team be created to determine whether SJA has not complied with its own policy or federal/provincial/territorial privacy legislation.

Reporting on the Investigation

1. Investigators will communicate the results of their investigation to the complainant in writing. This letter will also formally indicate that the matter is now considered closed by SJA.

2. The investigation team will submit a summary report to the privacy audit committee and to the Board of Directors of the respective jurisdiction. The complaint will be considered closed.
   2.1 As part of compliance and complaint monitoring, the summary report will be shared with the Privacy Compliance Team.

3. Complainants have the right to file a complaint with the provincial/territorial Privacy Commissioner of their respective jurisdiction at any time during the above complaint process.

Appeal Process

1. Complainants have the right to make one appeal of the final decision of the investigating team.

2. The complainant must submit a written appeal within 30 days of receiving formal written notification of the result of the investigation.
   - Appeals should be submitted directly to the local privacy audit committee.
   - The Privacy Audit Committee is only responsible for reviewing whether a decision made by the investigation team was based on material errors of fact or if the investigation team failed to follow the SJA procedures and /or processes described within this policy.

3. The decision by the committee will be final and binding. The complainant will be notified in writing of the final decision of the Privacy Audit Committee within 60 days of the initial appeal.

Privacy Toolkit

A toolkit has been developed to provide assistance in implementing the policy requirements. These tools are available on the SJA Intranet and include the following:

TOOL	PURPOSE
Collection Tool/Privacy Stmt Worksheet	To identify a sample privacy statement for forms commonly used by SJA.
Consent Form for the Release of Personal Information	To request an individual to consent to the release of his/her personal information to a third party
Council Implementation Guidelines by Department	To provide an outline of departmental responsibilities for the implementation of the SJA Privacy Policy
Policy Directional Statement - Approved Priory Council	To formalize the request for the development of a Privacy Policy from Priory Council to the National Management Team and provide an outline of the 10 privacy principles adopted by PIPEDA.
PP0104-Employee Benefits	To receive consent from employees to forward their personal information to a third party for the purpose of receiving employee benefits
Privacy Acts Across Canada	To provide members with a summary of the various privacy acts across Canada
Privacy Officer - Duties	To provide a summary of the responsibilities of a Privacy Officer.
SJA Privacy Policy [Compliance] Sign Off Sheet	To ensure that volunteers, staff, and instructors have read and understood their obligations within the SJA Privacy Policy
SJA Privacy Policy Statement - Corporate Clients	To be provided to corporate clients
SJA Privacy Policy Statement - Event Sponsors	To be provided to event sponsors
SJA Privacy Policy Statement - SJA Members	To be provided to members
SJA Privacy Policy Statement - Students	To be provided to students
Privacy Q & A	To provide answers to common privacy questions.
Retention Schedule	To provide guidelines to members for the record retention
SJA Privacy Policy	To be provided to any individual on request.
SJA Privacy Policy:Training Presentation	To assist in the education of volunteers, instructors and employees of the SJA Privacy Policy
Understanding Bill C6 - PIPEDA: Training Presentation	To assist in the education of volunteers, instructors and employees of PIPEDA

The toolkit is continually evolving to assist in the implementation of the SJA Privacy Policy and are subject to change. Members should review this section on the SJA internet at least once every three months.

Resources

PIPEDA - www.privcom.gc.ca/legislation/index_e_asp
Records Management Policy
Privacy Commissioners of Canada's – www.privcom.gc.ca

Policy Review

This policy will be reviewed every 3 years and as required.

STATEMENT OF COMPLIANCE FORM

St. John Ambulance is committed to protecting the accuracy, confidentiality and privacy of information and to adhering to all legislative requirements respecting the privacy of personal information. All employees, instructors, volunteers and other members who work, volunteer and/or are contracted by St. John Ambulance and who have access to personal information as a means of carrying out their duties and/or delivery of training and community services have a moral and legal obligation to protect an individual's personal information.

I, understand, accept, and will abide by the St. John Ambulance Privacy Policy. I understand that any violation of this policy is unethical and may constitute a criminal offense. Should I commit any violation to the St. John Ambulance Privacy Policy, I understand that my privileges may be revoked; and disciplinary and/or appropriate legal action may be taken.

_____

Name (Please Print)

_____

Signature Date: MM/DD/YY

Note: The signed form is to be retained on the personnel file and added as an activity to UNITY.