St. John Ambulance Saint-Jean

RECORDS MANAGEMENT POLICY

Policy Objective	The Records Management Policy is intended to ensure the safeguarding and protection of all records, in both paper and electronic format, to comply with applicable legislation.
Policy Statement	It is the policy of St. John Ambulance to safeguard and protect all records stored on-site or offsite, or records accessible to third party providers regardless of the format.
Effective Date	April 2006
Applies To	All volunteers, instructors, and employees in all departments, at all locations and for all records within the control of St. John Ambulance.

Policy Context

As part of the delivery of Community Services Programs and first aid training programs, St. John Ambulance (SJA) has within its control, records of various types and formats that relate directly to both personal information and corporate information.

Definitions

Active Record – a record that is still in use. Active records are to be maintained on-site within an SJA office in its appropriate department.

Archives – Materials created or received by a person, family or organization, public or private, in the conduct of their affairs and preserved because of the enduring value contained in the information or as evidence of the functions and responsibilities of their creator.

Artifacts – A man-made physical object, an item of natural origin or an item that is a representative example of class. Artifacts may be preserved as records, documenting a design or function.

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

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

Database – a collection of data arranged for ease and speed of search and retrieval.

Destroy – to remove any trace of information through various means, including erasing, shredding, and the like.

Destruction – the deletion of records beyond reconstruction.

Donor - one who contributes, in-kind or monetarily, to St. John Ambulance.

Electronic Records – Records that are implemented on or controlled by a computer or computer network.

Erase – to remove from electronic storage systems information

File – A record containing a document or documents relating to a specific topic.

Financial Records – Records relating to the Finance Department. These records may include invoices, receipts, bank statements etc…

Glean – to review and pull unnecessary or duplication of information for shredding

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.

Human Resources Records – Records concerning personnel recruitment and management

Indefinite Records – Records that are to be kept for an undetermined amount of time.

Inactive Record – Records that are no longer referenced and can be considered closed. These files are to be stored in a secure location and destroyed based on SJA's retention Schedule.

Jurisdiction – refers to the St. John Ambulance Councils and their respective operating centres (branches), and any community service divisions, units, fellowships, instructors that may be within their respective.
Legal Records – Records pertaining to Legal documentation, transactions, opinions, findings, determinations etc.

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

Off-site Storage – the storage of records, off of SJA property and usually by a third party provider.

On-site Storage – the storage of records on SJA property.

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. St. John Ambulance 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 St. John Ambulance as an organization operating across Canada
- information that is collected, used or disclosed by St. John Ambulance 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, employees) and clients.

- information in all formats including paper-based and electronic and in all locations.

PIPEDA – Personal Information Protection and Electronic Documents Act

Principles of Provenance – history of a document including author, approval bodies, etc.

Priory Council – Priory Council is the executive arm of Priory Chapter and derives its authority from the Prior of the Order. Priory Council, as a "board", is concerned with governance policy issues, and is invested with the power to authorize action in the name of Priory Chapter.

Record – any form of recorded information, kept in both electronic and paper format including: any correspondence, memorandum, report, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, documentary material, film, microform, sound recording, videotape, file or box containing any of the above.

Retention Schedule – a list of all record classes and the respective time periods for which they are kept and the required method of destruction.

Shred – to destroy

Third Party Supplier — a third party is a company or organization that has been contracted by St. John Ambulance 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 administration.

Policy Requirements

1. Records must be accurate and up to date.

2. Records are kept in a safe and secure location to protect against loss or theft.

3. Records must be retained for the time required to achieve the purpose for which they were collected.

4. Records must be protected against loss, theft and safeguarded from unauthorized access by implementing security safeguards appropriate to the sensitivity of the information regardless of the format in which it is held.

5. Records must be assigned to a record retention schedule, as per applicable federal and provincial legislation.

Responsibilities/Accountabilities

The National Office is responsible for:

- Acting in an advisory and support role for Provincial/Territorial Councils and Offices.
- Developing general policy and procedures related to records management.
- Training new members.
- Implementation and monitoring of the Records Management programme.

Provincial/Territorial Councils and Offices are responsible for:

- Acting in an advisory and support role for local SJA offices.
- Application of the general policy and procedures related to records management and related policies are required within their jurisdiction by law.
- Training new members.
- Implementation and monitoring of the Records Management programme.

Local SJA Offices are responsible for

- Application of the general policy and procedures related to records management and related policy as provided by their Provincial/Territorial Council
- Training new members.
- Implementation and monitoring of the Records Management programme.

Procedures

Records Management

In order to ensure that the information is maintained, accurate and up to date, each Council is required to develop an internal schedule to review their records management system. This includes a minimum annual review of records filing system, file locations and file contents to glean (remove duplicate information) and destroy (permanently remove).

Hard Copy

1. All records are to be maintained in a file with a title corresponding to the records in the file. The file codes for records are maintained by each Local SJA Offices and Council in a manner that is accessible and can be easily searched.
2. Records are to be safeguarded in a secure location.
3. A database of all records stored in hardcopy must be maintained and up to date for easy access and search ability.

Electronic Records

Policies relating to electronic records management such as the protection and storage of electronic records are located herein. For policies relating to Acceptable Use, Intranet, Email, Website and the like, refer to the Information Technology Services Policy.

1. Server Information
    1.2. All information located on the server is the property of, and under the control of, St. John Ambulance. All servers and computer stations must be password protected whereby passwords are updated on a quarterly basis.
    1.3. For easy accessibility and search requirements, all electronic records should be organized on the server in a logical manner (by year, and department and/or subject). Records must be reviewed on a yearly basis for consolidation and organization.
    1.4. Back-ups are performed on a regular basis by a designated individual, IT or external third party. Yearly back-ups are to be retained in a zip file in a secure location for seven years.
    1.5. Retention - Records are to be retained on-site in a permanent format (e.g. either DVD, CD or other retrievable means) for three years after which they are kept for an additional four years in storage (can be off-site).

2. Software Upgrades - All electronic records should be converted when there is a software upgrade. Quality check should be performed after conversion to ensure data has not been corrupted during the process. Date and format are to be indicated.

3. Recordings - Recordings for the purpose of collecting information for minutes may be done by cassette tape, digital voice recorders or computers. When recording meetings, all participants must be aware and permission must be received in advance of the meeting. This may be done annually or as new members join a Committee, Team and/or the like. Records of meetings are retained until minutes have been approved by the respectful committee at which time they are destroyed.

Other recordings for the purposes of marketing and communications must be saved electronically with the properties of the recording completed in full to include confirmation of permission to use as per the release form.

4. Digital Images and Photos - All digital images and photos should be approved and be able to provide proof of approval for use prior to uploading to a server, computer, website or to be used in marketing collateral materials, and the like.

   A signed photo/image release and/or permission form should be stored in a secure location for future reference, as required.

   It is recommended that images/photos saved in electronic format should include a summary in the properties section of the file (in Windows, select File and then select "Properties", then select the tab entitled "Summary").

   For the purposes of storage and future use of photos / image, the file should be saved for print quality (high resolution or minimum 300 dpi) and/or web quality *low resolution or between 72 dpi – 299 dpi).

5. E-mail
   All information located on the server is the property of, and under the control of, St. John Ambulance. Subsequently an email account provided to a member of SJA is an electronic record and should be treated accordingly.

   Emails should be reviewed and auto-archived on a monthly basis. The Archive folder should be kept in a secure location on the server and reviewed on a yearly basis.

   Every 3 years archive folders shall be backed up on a zip drive and stored at a secure location.

Archival and Historical Records
Archival records should be stored in a safe and environmentally controlled location, and are permanent records for the purpose of protecting and preserving the organization's history. Subject to the archival type, archival records are to be stored at a specific temperature and humidity level.

UNITY
Specific requirements to record management are included in Attachment B.

Security Access
Based upon the personal and confidential information contained within a record, access to records will be restricted. The following security access level is to be applied to records: (see records retention schedule).

1. Security Level for Internal Use
   The following is a classification of information according to its sensitivity and the related protection that is required:
   Level 2 – Securely protected, locked cabinet, restricted access and access to designated personnel access
   Level 1 – Securely protected, locked cabinet, limited personnel access
   Level 0 – Contains no personal information, securely protected location

Onsite/Offsite Storage of Records
Records must be stored in a records file with the following information.

1. Box number
2. Department
3. 'From' Date and 'To' Date
4. Major Description
5. Destruction Date, if applicable

Destruction Approval
Destruction dates of all records must be monitored for compliance with national, federal and provincial laws. All records designated for destruction shall receive a request from the department head to confirm the date of destruction. A copy of the request, approving destruction, must be signed by the Department Director prior to issuing the directive to the assigned/designated individual responsible for monitoring and complying with the Records Management Policy. Confirmation of the destruction is required and may be shown by signature or certification of destruction, i.e. by a third party supplier.

Resources
Changes to resources identified below may directly impact the procedures contained herein:
SJA Privacy Policy
Personal Information Protection & Electronic Documents Act (PIPEDA)

Policy Review
The Records Management Policy should be reviewed every 3 years, and as required.

Attachment A

Record Retention Schedule

*Within the Privacy Policy, St. John Ambulance refers to areas where records are securely located: National Office **(NO)** and its provincial and territorial councils (**CO**) and their respective operating centres (branches)(**BR**). Hard Copy or Paper Records no longer valid are gleaned (the process of reviewing and extracting pertinent information) and destroyed (non-pertinent information). Soft Copy Records or Electronic Records are gleaned and moved to a secure electronic storage site.*

Security Level for Internal Use:

Level 2 – Securely protected, locked cabinet, restricted access and access to designated personnel access

Level 1 – Securely protected, locked cabinet, limited personnel access

Level 0 – Contains no personal information, securely protected location

Record Description	Format	Area where records are held	Retention Schedule	Method of Disposal	Security Level
Training Records					
Registration Forms	Paper Electronically	NO, CO, BR NO, CO, BR	Glean/move 3 years	Destroy/Shred Erase	2
Instructor Applications / Instructor-Trainer Applications	Paper application Electronically	NO, CO, BR NO, CO, BR	Glean/move 3 years (post dep.)	Destroy/Shred Glean/Erase	2
Instructor agreements	Paper	CO, BR	Indefinitely	Glean/Shred	1
Instructor Monitoring Reports	Paper Electronically	NO, CO, BR	Glean/Move Glean/Move	Destroy/Shred Erase	2
Course Survey	Paper	CO,BR	Glean/Move	Glean/Shred	0
Volunteer/ Community Services Records					
Applications	Paper	NO, CO, BR	Glean/move	Destroy/Shred	2
Police checks/ Attestation Forms	Electronically Paper	CO, BR NO, CO, BR	7 years (post dep.) 7 years (post dep.)	Glean/Erase Glean/Shred	2
Patient/care records	Paper	CO, BR	10 years	Glean/Shred	2
Volunteer Personal Information	Paper Electronically	NO, CO, BR NO, CO, BR	Glean/move Indefinitely	Destroy/Shred Glean/Shred	2
Performance records	Paper Electronically	CO, BR	7 years (post dep.) 7 years (post dep.)	Glean/Shred Glean/Erase	2

Record Description	Format	Area where records are held	Retention Schedule	Method of Disposal	Security Level
Grievance disputes	Paper Electronically	NO, CO, BR	7 years (post dep.) 7 years (post dep.)	Glean/Shred Glean/Erase	2
Member service records / Promotions in the Order	Paper Electronically	NO, CO, BR NO. CO, BR	Glean/move Indefinitely	Destroy/Shred Glean/Erase	2
Nominations Forms	Paper Electronically	NO, CO	2 years 2 years	Destroy/Shred Erase	2
Awards	Paper Electronically	NO, CO, BR NO. CO, BR	Glean/move Indefinitely	Destroy/Shred Glean/Erase	1
Bursary Applications (recipients)	Paper	NO, CO	10 years	Destroy/Shred	2
Bursary Applications (non-recipients)	Paper	NO, CO	2 years	Destroy/Shred	2
Fundraising/ Donations					
Receipts	Paper	NO, CO, BR	3 years	Destroy/Shred	1
Records of donations subject to direction by donor	Paper	NO, CO, BR	Indefinitely	Historical Record	1
Property	Paper	NO. CO, BR	Indefinitely	Historical Record	1
Administration					
Personnel Records	Paper Electronically	NO, CO, BR NO, CO, BR	7 years (post dep) 7 years (post dep.)	Glean/Shred Glean/Erase	2
Payroll	Paper Electronically	NO, CO, BR NO, CO, BR	7 years 7 years	Glean/Shred Glean/Erase	2
Source deduction forms	Paper	NO, CO, BR	7 years	Glean Shred	2
Time Sheets	Electronically Paper	NO, CO, BR NO, CO, BR	7 years 7 years	Glean/Shred Glean/Erase	1
New/Change forms: Pension Group Insurance	Paper or Electronically	NO, CO, BR NO, CO, BR	7 years 7 years	Glean/Shred Glean/Erase	2
Board and Committee Meeting Minutes	Paper or Electronically	NO, CO, BR NO, CO, BR	7 years Indefinitely	Glean/Shred Historical	0

Record Description	Format	Area where records are held	Retention Schedule	Method of Disposal	Security Level
Constitution/ Bylaws	Paper	NO, CO	Indefinitely	Historical	0
Building/site contracts/titles/ environmental studies	Paper	NO, CO	Indefinitely	Historical	1
Trademarks and copyright applications	Paper	NO, CO	Indefinitely	Historical	1
Records relating to legal issues	Paper Electronic	NO, CO, BR	25 years	Glean/Shred Glean/Erase	2
Financial The General Ledger and other book of final entry containing the summaries of the year-to-year transactions and all Source Documents	Paper Electronically	NO, CO NO, CO	7 years 7 years	Glean/Shred Glean/Erase	1
Audited Financial Statements	Paper Electronic	NO, CO, BR NO, CO, BR	7 years 7 years	Glean/Shred Glean/Erase	0

Retention Schedule Sources: CCRA, HRDC, CPSO, CNO
(Post. Dep.) refers to post departure.

For questions and/or changes concerning the Retention Schedule, please contact the CEO or Executive Director of your Provincial / Territorial Council. For questions regarding St. John Ambulance's Privacy Policy, email the privacyofficer@sja.ca or contact the Privacy Officer for St. John Ambulance Provincial / Territorial Office in your jurisdiction.

Attachment B

Records Management - UNITY

Access
Only those users who have been approved and licensed by the Provincial/Territorial UNITY Team Lead will have access to UNITY.

Visibility
Within UNITY, *visibility* refers to the limiting of the views or screens seen by users as well as the records seen by users.

Access to UNITY Screens and Views:
There is a first level security within UNITY that is based on each users individual roles and responsibilities. UNITY defines what roles see what screens and views and therefore your system might look different than your colleagues.

Access to UNITY Data
Another level of security is limiting access to UNITY data. Each user within the system is tagged to an Organizational Unit (Org Unit) ie. Council, Branch, Admin Centre. As well, each piece of UNITY data (Contact, Account) is also tagged to an Org Unit. In certain cases, UNITY will match the data to your Org Unit to determine whether you have rights to update the information. The following table outlines the security levels placed on each major module of the system along with a narrative describing the reason for the decisions.

Legend for the Visibility Levels

All	All employees across the country are granted this right.
Branch	All employees within a branch are granted the particular right. These rights also extend to parent Admin Centres or Councils of a branch who will always have at least the same rights of a branch.
Council	All Council employees will be provided the rights but not branch or admin centre employees.
National	All employees at National Office are granted the particular right.

(*)	Implies that a particular right extends only to those records that have been created by that user's organizational unit but not other records. For example, if an Update: All(*) implies that a user may only update records that they created and may not update records that another branch has created.

UNITY User Requirements

a) All users must be approved by the respective Council
b) All users must be trained in the Privacy Policy.
c) All default passwords provided to users should be changed.
d) All users must receive training from a current UNITY user/employees member respective of their business function within SJA.
e) Training / Communications
    i) A UNITY reference guide is available to all new users and is available on the intranet. All updates are added as required.
    ii) A monthly newsletter is sent to all users regarding any updates, changes or crucial information via email from the National Office.
    iii) Continual online training is available to all councils upon request to the National Office.