Information Management for Conferences & Councils by Laws & in Practice

Society of Saint Vincent de Paul (SSVP)

The information management of the Society Of Saint Vincent de Paul, at all levels, is driven by requirements established by government, industry best practices and the Society.

2019-06-20

Why? To Help Members Clarify and Understand.

With the reality of **inappropriate access of personal data** in our social environment, there is a **duty to protect against misuse** of information for purposes such as identity theft.

- Protects Personal Information
- Protects Society's reputation and charitable status

- Personal Information Protection
  - Extend current best practices demonstrated by the Rule and Statutes and the Operations Manual.
- Proper Management of the Society's Information
  - Assists in proper and accurate reporting within the Society and to governments.

Note: **All presented is a working Draft.**

Even with this presentation is labelled as a **“draft”, it is imperative that information always be protected and best practices be implemented.** This is not a reflection of a change from what already exists in the Rule and Statutes.

Who

Committee:

- Richard Pommainville, Executive Director SSVP Ottawa ON
- Ken McClintock Vincentian, Halifax NS
- Mary Dunnigan Vincentian, Edmonton AB
- Robert Graham Vincentian, Courtice ON (Near Oshawa)

Approach

- **Crafted SSVP Principles** based on the principles Canadian Government Personal Information Protection and Electronic Documents Act (PIPEDA);
- **Skimmed PIPEDA** and discussed sections and approaches highlighted by Government website;
- **Reviewed** Provincial Privacy Acts **for jurisdiction over charities** – no in depth investigation;
- Discussed relevant parts of the **Rule;**
- Consulted with **lawyer** on some of the Q&A questions;
- Researched Canada Revenue Agency **(CRA)** Requirements;
- Researched industry **best practices;**
- Drew from **personal experience.**

Pre-amble:

The following privacy and security Information Management (IM) principles for the Society of Saint Vincent de Paul (SSVP) apply to **all information collected and used by those acting on behalf of the Society,** regardless of how it is recorded, including as **knowledge, as hard copy or on digital media.** The Society's principles leverage the Canadian Government Personal Information Protection and Electronic Documents Act (PIPEDA), and parallel provincial statutes and Canada Revenue Agency (CRA) requirements. Consideration is required related to information of **our clients, volunteers, members, employees and donors, and other Society operational information such as financial, minutes, reports, statistics.**

SSVP Information Management (IM) Principles (Draft)

Principle 1 - Accountability

The Society of Saint Vincent de Paul, at all levels, is responsible for personal and operational information under its control. Each president is accountable and shall appoint someone to be responsible for compliance with these information principles and procedures.

SSVP Information Management (IM) Principles (Draft)

Principle 2 - Identifying Purposes

The purpose for which the personal information is being collected must be identified by the organization before or at the time of collection. Notify the individual, either orally or in writing, of these purposes.

SSVP Information Management (IM) Principles (Draft)

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate (see PIPEDA Paragraphs 7(3) (d.1) and 7(3) (d.2))*

Verbal consent may be all that is required, but it should be recorded.

Where there is an intention to disclose personal information to third parties or any other secondary purpose that Households would not reasonably be aware, then written consent shall be obtained.

* source https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

SSVP Information Management (IM) Principles (Draft)

Principle 4 - Limiting Collection

The collection of personal information must be limited to that which is needed by the Society and is necessary for the identified purposes. Information must be collected by fair and lawful means. In general, sensitive personal information should not be collected.

(please refer to Questions & Answers section for more explicit description around collection of Sensitive Personal Information (SPI)).

SSVP Information Management (IM) Principles (Draft)

Principle 5 - Limiting Use, Disclosure, and Retention

Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Sensitive information always needs privacy protection during conversations or sharing by taking into consideration the who, what, where, when, why and how.

SSVP Information Management (IM) Principles (Draft)

Principle 6 - Accuracy

Personal and operational information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the intent for which it is to be used.

SSVP Information Management (IM) Principles (Draft)

Principle 7 - Safeguards

Personal and operational information must be protected by appropriate security relative to the sensitivity of the information; it must cover:

- Knowledge (e.g. information learned);
- Hard Copy (e.g. paper);
- Digital (e.g. Excel spreadsheet, online storage).

SSVP Information Management (IM) Principles (Draft)

Principle 8 - Openness

SSVP, at all levels, must be prepared to provide information about its policies and practices relating to the management of personal information. This approach is in line with policies and practices as reflected on the National web site, www.ssvp.ca

SSVP Information Management (IM) Principles (Draft)

Principle 9 - Individual Access

Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. This principle is aligned to Principle #3 “Consent”.

SSVP Information Management (IM) Principles (Draft)

Principle 10 - Challenging Compliance

An individual shall be able to challenge an organization's compliance with the above principles. The challenge should be addressed to the person accountable for the Society's information compliance.

Q & A. **Principle 1 - Accountability**

Q: What are the definitions of **“Accountable”** versus **“Responsible”** for application and implementation?

A: **Accountable:** the individual whose mandate is to **ensure policy and procedure** are in place. **Responsible:** the individual who will **implement and apply** the associated procedure for adherence to the policy. In some instances, they could be the same individual but likely are different individuals.

Q: Who is responsible for proper data management?

A: Ultimately, **everyone is responsible** to ensuring proper data management. For SSVP, this includes information concerning clients, volunteers, members, employees and donors; other Society’s operational information such as financial, minutes, reports, statistics, etc. may also require special provisions.

Q & A. **Principle 1 - Accountability**

Q: Who is bound by the **Personal Information Protection and Electronic Documents Act** (PIPEDA)?

A: Even if some non-profit organizations are not subject to the Act because they do not engage in commercial activities, it is **good practice** to have policies and procedures to protect information.

Unless they are engaging in commercial activities that are not central to their mandate and involve personal information, PIPEDA does not generally apply to not-for-profit and charity groups.

Reference sources:

- https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_19/
- https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/

Q & A. **Principle 1 - Accountability**

Q: For the proper data management of privacy and security, to whom is SSVP accountable and responsible?

A: SSVP is accountable and responsible **to those whom the principles protect.** SSVP needs to adhere to **government regulations.** Plus, it is **good ethical practice** to ensure personal information is properly secured.

Q & A. **Principle 1 - Accountability**

Q: Which Provincial Privacy Acts impact SSVP and how?

A: There are variations from province to province. Provincial legislation officially deemed **similar** can be seen at (all not including Saskatchewan, Manitoba, PEI or Territories)

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/provincial-legislation-deemed-substantially-similar-to-pipeda/

Q: Which **Provincial Privacy Acts include charities?**

A: Please consult your respective provincial acts for further details. Additional details in the appendix of the policy will be provided.

e.g.

- For **British Columbia**, refer to Section 2: http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01
- For **Quebec**, refer to Division 1, Sections 17-24: http://www.legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1

Q & A. **Principle 2 - Identifying Purposes**

- **Record all identified purposes** for easy reference in case someone requests an account of such information. Ensure that these **purposes are limited** to what a reasonable person would expect under the circumstances.
- Define your purposes for **collecting data as clearly and narrowly as possible** so people can understand how the information will be used or disclosed.

Examples of purposes include:

- Verifying details for level of assistance and follow-up;
- Maintaining records of assistance so as to comply with Conference policy;
- Processing a rebate form;
- Advocating on family's behalf.

Q & A. **Principle 3 - Consent**

- The Society considers that all **information** collected from **Households is personal** and, in some cases, **sensitive**. Accordingly, the Society requires that **consent be obtained in all cases** where personal information is collected by the Council/Conference. Consent shall be **explicit**, which can be obtained either **orally or in writing** (this is called express consent under PIPEDA).
- Where there is an intention **to disclose personal information** to third parties or any other secondary purpose that Households would not reasonably be aware, then written consent must be obtained.
- In some cases, consent is not necessary, such as when information is being disclosed for the detection and prevention of fraud or to support law enforcement.
- Collection of personal information includes **discussion** where personal information is provided, **regardless of physical retention.**
- **A record of the consent,** including date and members present, shall be retained by Conferences and Councils.

Q & A. **Principle 3 - Consent**

Q: For using pictures or videos of people, is consent required from an individual?

A: **In every case,** it is important to obtain the individual consent, and if children under 18 are engaged, then their parent's consent.
(Note: based on consultation with a lawyer)

Implicit consent notification at events can be demonstrated by posting at registration, online or at registration desk; attendees need to notify organizers they do not want to have their pictures taken.

Q & A. **Principle 3 - Consent**

Q: Should email communications **include a confidentiality statement**?

A: For Society communication, it would be **advisable** to have a statement in the signature such as:

> Confidential: This email and any attachments transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the sender and delete the email immediately. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Q & A. **Principle 4 - Limiting Collection**

- Identify the kind of personal information **normally required** in policies and practices and ensure all volunteers are familiar with them. **Collecting less information** also reduces the risks associated with unauthorized disclosures.
- **Sensitive Personal Information (SPI)** is defined as information that if **lost, compromised, or disclosed** could result in substantial **harm**, embarrassment, inconvenience, or unfairness to an individual.
- Although under some circumstances it may be necessary to collect SPI, in general, Society members **should not collect the SPI identified below:** -

- Social Insurance Numbers (SIN); - Bank account numbers; - Health Card number;

- Healthcare related information; - Student ID information; - Medical insurance information;

- Credit and debit card numbers; - Drivers license number; - Medical records;

-Passport /Citizenship information; -Financial records.

Keep in mind that **any information can be sensitive**, depending on the context.

Q & A. **Principle 4 - Limiting Collection**

Q: Should the birthdate be collected?

A: As an extension of the principle #2 (identifying purpose), the **actual birthdate** is **not really relevant** for the work of the Society; however, the **birth year** can assist when interacting for certain social programs, especially youth.

Q & A. **Principle 4 - Limiting Collection**

Q: What information do you put in a consent form?

A: The collection of personal information must be limited to that which is **needed** by the Society and is necessary for the identified purposes. Information must be collected by **fair and lawful means.**

Q: What **guidelines** should be followed when collecting information to perform your charitable work?

A: Items for considerations:

- **Think safety** – need to know what is happening or previously happened before visit or interaction;
- **Think caring** – can interact better, be personable and sometimes anticipate needs -better ask questions to help; limited history
- **Think proof** – logs of charitable actions; decisions in minutes etc.

Q & A. **Principle 4 - Limiting Collection**

Q: When contemplating safety, **what level** of Police Records Check (PRC) should be **collected from members** to verify their authorization to have client contact and collect personal client information:

A: There are three levels to consider:

Level 1--*Criminal Record Check (CRC)* *This check is intended for applicants who are involved as a volunteer, employee or in any situation where a basic CRC is requested (e.g., retail or immigration).* This check is NOT intended for applicants who are seeking volunteer and/or employment with vulnerable persons (see Level 3 below).

Level 2--*Criminal Record and Judicial Matters Check (CRJM) Similar to Level 1 and includes charges before the courts – not yet convicted.*

Level 3--*Vulnerable Sector Check (VSC)* *This check is restricted to applicants seeking employment and/or volunteering in a position of authority or trust relative to vulnerable persons in Canada only.*

All members including auxiliary members of the Society are required to have a PRC with a Vulnerable Sector Check (VSC).

Q & A. **Principle 4 - Limiting Collection**

Q: What does **'Vulnerable Sector'** mean?

A: As defined by the **Criminal Record Act:** *"vulnerable sector" means persons who are in a* **position of dependence** *on others or are otherwise at a* **greater risk than the general population,** *of being harmed by persons in authority or trust to them. A person's* **age, disability, or other circumstances** *(whether temporary or permanent), can make someone vulnerable. Children, as defined by the Criminal Record Act, means persons who are less than 18 years of age.*

Q & A. **Principle 4 - Limiting Collection**

Q: What is the **Society's policy** with respect to Police Records Checks (PRC)?

A: Currently, as reflected in the **Operations Manual (9.11** Service Covenant/Confidentiality Agreement), all members of the Society are required to have a PRC with a Vulnerable Sector Check (VSC) every three (3) years.

Q & A. **Principle 5 - Limiting Use, Disclosure, and Retention**

- Sensitive information always needs privacy protection during conversations or sharing by taking into consideration the **who, what, where, when, why and how.**

- Note that the Society of Saint Vincent de Paul **will not disclose personal information** to third parties **without consent.**

- Note that the Society of Saint Vincent de Paul **will not trade, sell or rent personal information to third parties.**

Office of the Privacy Commissioner of Canada Consent Guidelines:
https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805

Q & A. **Principle 5 - Limiting Use, Disclosure, and Retention**

Q: How may we **protect the identity** of Vincentians when contacting clients?

A:

- using **codes** in front of phone numbers when dialing such as *67 (landline) #31(cell)
- calling from a **Society of Saint Vincent de Paul phone or a parish office phone.**
- only using **first name.**

Q: How do we protect hard copy information?

A:

- securely **locked** space
- during **transport** safeguard from **loss or unauthorized access**
- **not recognizable after destruction** – example: cross cut shredding
- **accessible to at least one secondary person** in case the primary responsible person becomes incapacitated or unavailable.
- organized and stored for **ease of transfer** during succession.

Q & A. **Principle 5 - Limiting Use, Disclosure, and Retention**

Section 3.15 Rule and Statutes Update

Non-incorporated conferences or councils				
Documents	Time Kept			
	3 years	3 years past the end of the term of that president	6 years	In perpetuity
Aggregation, institution, or twinning forms				X
Membership application forms				X
Canada Revenue Agency: charitable registration forms				X
Minutes of meetings				X
Financial records			X	
Lists of members of the boards of directors				X
General correspondence during the mandate of any president		X		
Case records	X			
Annual reports				X
Proxies during the mandate of any president		X		

Q & A. **Principle 5 - Limiting Use, Disclosure, and Retention**

Q: In section 3.15 of the Rule and Statutes (Retention and Archiving of Records), what is covered **"General Correspondence during the mandate of a President"?**

A**: Any correspondence related to the work of conferences or councils is considered correspondence.** Usually there is a motion in the minutes to receive and file correspondence. However, when it pertains to the dispensation of **funds,** or required activities, this is usually kept then for **seven years,** just as for finance records.

Q: How and for how long do you retain paper documents? If you scan / take picture of document, can you destroy paper copy? If client information is collected, but client has not been served for many years, what is the process to remove (/clean) the documents **(All media)**?

A: Client information **must be destroyed after three (3) years after the information has been obtained.** Three (3) years is a good period as any longer increases the risk of non-authorized information being divulged; by extension, if destroyed, it does provide a good measure to reflect the confidential nature of the information.

Note: A lawyer was consulted for this question.

Q & A. **Principle 5 - Limiting Use, Disclosure, and Retention**

Q: How do we get that financial information must be kept for 7 years?

A: CRA Financial Data Six Year Rule points to the **current year + 6 full years** leading to the 7 years.

In CRA document IC78-10r5-10e, refer to section 26 & 27 -28 + appendix:
https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/keeping-records/where-keep-your-records-long-request-permission-destroy-them-early.html

---

Q: Are there any known exceptions to the CRA rule to keep financial records longer than 6 full years?

A: Yes, in the event that a donor directs a donation, be it a monetary donation or in kind, has a special purpose or restrictions on its use, then the **directive instructions and the tax receipt copy needs to be kept on record for a period of not less than 10 years.** E.g. A donor donates money or land and indicates it needs to be applied to Special Works: Examples a shelter, a store or housing.

Please refer to CRA document IC78-10r5-10e 5800 (1) (d) (iv).

Q & A. **Principle 6 - Accuracy**

Q: Is it necessary for a client to show government issued documentation when we visit a client?

A: Although not a requirement, but as a practise, this helps ensure accuracy.

Q & A. **Principle 6 - Accuracy**

Q: For members, there are **many forms** from the **Operations Manual** to fill as part of the **screening and adhesion**; is there a **rationalization** for all the forms?

A: It is important to keep these documents **relevant and accurate** and to report to assemblies and council presidents of the importance to remind members that there are either **government regulations to meet or insurance requirements.**

From the Operations Manual, key forms are:

- 9.9 Screening – Membership Application
- 9.10 Screening – Interview checklist/Reference Check Report
- 9.11 Screening – Member Service Covenant/Confidentiality Agreement
- 9.23 Abuse, Discrimination and Harassment Prevention Checklist and Acknowledgement

Q & A. **Principle 7 - Safeguards**

Safeguards must be in place to cover the approach used to **gather and transport** information:

- Knowledge (e.g. information learned);
- Hard Copy (e.g. paper);
- Digital (e.g. Excel spreadsheet, online storage).

Knowledge and Hard Copy were covered in Principle 5 - Limiting Use, Disclosure, and Retention .

Q & A. **Principle 7 - Safeguards**

Q: Are there guidelines when using third party services?

A:

- no system is immune to **hacking;**
- third party online storage services and systems need to be **evaluated;**
  - **support** the Society's information **management principles;**
  - accomplished through **research** and interview;
  - **who not of the Society** has access;
  - does the provider have **good privacy principles and practices** to protect its clients;
  - services to **multiple organizational entities** within a hierarchical structure (e.g. several Conferences & Councils) appropriate **controls** should be in place to **restrict access** to only that information **required** for that organizational entity;
    - levels of permission;
    - clear access points for each user;
      - ensure confidentiality;
      - reduce the exposure in the event of a breach.

Q & A. **Principle 7 - Safeguards**

A: For online storage:

- Personal information records must be kept on a **Canadian server**.
- Master copies of the financial records, according to Canadian Revenue Agency (CRA) rules must be kept in Canada. Backups do not have to be stored in Canada;
- Other information may be stored elsewhere online;
- A plan needs to be in place and actioned to **avoid loss** of access to an account or loss of data within the account **because of lack of use.** e.g. Outdated information or accounts may end up be **erased by third party providers.**

Q & A. **Principle 7 - Safeguards**

Q: What are the security measures which have to be in place?

A: Backups:

- **arranged and be frequent** to **continue operations** without loss of accurate records or a major effort to reconstruct.
- **one backup kept fully intact offsite until it is replaced** by the most recent backup of the master digital information
- three copies to be managed: the master, the offsite backup and the recently created backup to be switched with the offsite backup

Q & A. **Principle 7 - Safeguards**

A: Password Policy

Techniques such as strong passwords, limitation of distribution of passwords and regular changing of passwords are best practice.

- Note '**Strong Character Passwords**' in the definition section of the handout.
- Passwords include Personal Identification Numbers (PIN) and Safe Combinations;
- Information protected by passwords, encryption or other methods must be **accessible** by at least one **secondary member** in case the primary responsible member is **incapacitated** or unavailable.

Applicable to:

- Web sites
- Safes
- Cell Phones
- Voice Mail
- Logons to computers where the information is stored.

Q & A. **Principle 7 - Safeguards**

Other Actions:

- **changing password** when members leave;
- Use of encryption;
- **Sensitive information** transported via email, or memory key must be **password protected or encrypted;**
- To minimize, the proliferation of protected documents by old passwords, when documents are **on a protected media** or computer system, the individual **documents should be unprotected;**
- **Two-Step Authentication** is expected to become **more widely used in the future and depending upon the circumstances, this method should be considered;**
- On personal computers, **keep Society data separate from your own personal data**
  - Possible option – backed up memory sticks.

Q & A. **Principle 7 - Safeguards**

Q: Do **primary financial online records** have to be kept in Canada?

A: Yes, the server has to physically be located **in Canada.** Please refer to Canada Revenue Agency (CRA) under the heading "Where to keep your records."

- https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/keeping-records/where-keep-your-records-long-request-permission-destroy-them-early.html

---

Q: What type of media do electronically issued donation receipts need to be stored on?

A: To protect computer-generated receipts from unauthorized access(fraud), registered charities should ensure that:

- the computer system used to store the receipts is password protected and restricts entry to and modification of donor contribution records;
- donor records are stored on **non-erasable media**, such as CD-ROMs or printouts, with copies kept off-site for recovery purposes;
- hard copies of issued receipts can be printed on request

Please refer to Canada Revenue Agency (CRA)

- https://www.canada.ca/en/revenue-agency/services/charities-giving/charities/operating-a-registered-charity/issuing-receipts/computer-generated-receipts.html

Q & A. **Principle 7 - Safeguards**

A: Organization redundancy

- In order to initiate and **continue future long-term digital management of information,** plans must ensure those responsible have the necessary level of **computer literacy, experience and skills.** Need to avoid digital management of information practices which has been **left by departing members for less experienced members to manage.**

- Information should be **organized and stored** to allow for **ease of transfer** during officer transitions;

- After the transfer of information and successful **transition** depending upon the role of the outgoing member the **information should be removed from personal storage devices** except for the correspondence of the past president which follows a three-year retention rule.

Q & A. **Principle 8 - Openness**

Q: What is necessary for conferences and councils to do to ensure that the Information Management Principles of the Society are known?

A: SSVP, at **all levels,** must be **familiar with the policies and practices** relating to the management of personal information published on the **National web site**, and **share it when asked.**

- Canadian Rule and Statutes
- Operations Manual
- Website Pages

Q & A. **Principle 9 - Individual Access**

Q: Can any person on whom we have collected information ask to see that information?

A: **Yes,** and in a **timely manner,** the privacy officer or President's delegate will share this data.

Q & A. **Principle 10 - Challenging Compliance**

Q: Who should be responsible to handle the compliance challenges?

A: The **appointed individual by the president** who has the responsibility as a privacy officer to **handle compliancy challenge** would be prime and has the responsibility to keep the President informed who is accountable.

What is next?

- **Please give feedback** and input to national@ssvp.ca regarding this presentation and its parallel policy document being posted at www.ssvp.ca. Please use 'Information Management' in the email subject line.
- The Operations Manual will be updated to include an Information Management policy to complement the existing policies.
- Go forth and mutliply the practise:

PROTECT THE INFORMATION OF CLIENTS, VOLUNTEERS, MEMBERS, EMPLOYEES AND DONORS, AND THE SOCIETY.