



Privacy, Retention of Personal Information

Last Reviewed: February 2026

Reviewed by: LFNP Contributors

Time to Read: 8 minutes

This Fact Sheet provides information about the legal rules non-profits should follow for keeping (retaining) personal information.

Most non-profits retain (keep) records of some kind. Typically, these records are in paper and/or digital/electronic form. Paper records include all records in a physical (non-electronic) form such as printed documents and emails and hand-written notes.

Digital/electronic records include all information recorded by a computer such as email messages, word processed documents, images, spreadsheets, and databases. Best practice is to ensure that both types of records are retained securely.

Paper Records	Digital/Electronic Records
Limit access: securely store paper records behind a locked door.	Encrypt (make data unreadable except by certain people using an authorized device) highly sensitive electronic records.
Secure sensitive personal information e.g., medical and financial, in a locked cabinet.	Password protect (only those with the assigned code, word, or phrase can access) records stored online or on shared drives.
Only provide keys to doors/cabinets to specific authorized individuals.	Use and regularly update antivirus software to protect electronic records from illegal access, sharing, and corruption.

Different types of records should be kept for different amounts of time. For example, financial records must be kept for 7 years and official records (under section 23 of the Societies Act) for 10 years.

Personal information should not be kept if it is no longer necessary for the purpose it was collected. For example, if a non-profit had people sign up for a newsletter and it stops publishing the newsletter, the names and email addresses of those who signed up are no

longer necessary. Those documents can be deleted or shredded as they are no longer relevant.