Privacy and Confidentiality Policy Statement

Oakville Meals on Wheels recognizes that every individual has a right to privacy. Oakville Meals on Wheels will protect privacy and personal information in a manner consistent with the public interest, applicable legislation, and personal safety.

Means

Oakville Meals on Wheels maintains policies, training and communication practices to ensure the confidentiality of every individual, including persons served, volunteers, and staff.

Personal information means information about an identifiable individual that is not publicly available. Information that is publicly available (for example, information published in a public directory or on an individual's professional profile) is not considered personal information for the purposes of this policy. Personal information includes any other information about a person, including but not limited to family/caregiver information, service requirements, applications, medical information, financial information, or consent forms.

Accountability

Oakville Meals on Wheels is responsible for protecting personal information and designates the Director of Operations as accountable for:

- control of records
- compliance with privacy policies and privacy legislation
- implementing procedures that protect personal information
- responding to complaints and inquiries

The Director of Operations will provide their name and contact information to anyone who has questions about the protection of personal information or who requests information about compliance with this policy.

Accuracy and Limitation
Personal information will be collected by fair and lawful means and will be:

- accurate and current as necessary for the purpose for which it is used
- limited to what is necessary for identified purposes that can be explained

The Director of Operations will implement procedures to ensure information is accurate and updated as required. Individuals will not be contacted to provide information unless doing so is required to fulfill a legitimate and ethical purpose that can be explained.

Challenging Compliance
Any individual may challenge compliance with this policy by contacting the Director of Operations.

Oakville Meals on Wheels will maintain procedures to receive and respond to complaints or inquiries related to the collection, use, retention, or disclosure of personal information. The Director of Operations will:

- inform individuals about relevant complaint and review mechanisms
- address and attempt to resolve complaints and inquiries
- evaluate internal and external review processes after each complaint and amend Oakville Meals on Wheels' policies and practices where necessary

Disclosure
Personal information will not be disclosed for purposes other than those for which it was collected, except as required or permitted by law.

A Confidentiality Agreement will be reviewed and signed by staff and volunteers during orientation.

Safeguards will be in place to ensure records are accessed only by authorized personnel. If a valid subpoena, search warrant, or court order is received, the Director of Operations will validate the request and comply as required. Staff and volunteers must immediately refer any such requests to the Director of Operations.

Where personal information is disclosed in an investigation or legal process, Oakville Meals on Wheels will document what information was provided, the date(s), to whom it was provided, and the reason.

Retention and Disposal

Personal information will be retained only as long as necessary to fulfill the purposes for which it was collected, generally according to the following guidelines:

- Client records: 7 years after the client ceases using Oakville Meals on Wheels' services
- Staff files: 7 years after the employee leaves Oakville Meals on Wheels
- Volunteer files: 3 years after the volunteer leaves Oakville Meals on Wheels
- Unprocessed employee/volunteer applications*****: 1 year after application
- Financial information: 7 years

*****_Employment applications submitted through third party recuritment platforms (e.g. LinkedIn) are reviewed within those platforms and are not retained by the orgnaization unless required for hiring or legal purposes._

Personal information will be stored in a secure, locked location when not in use. When in use, files and documents containing personal information will not be left open for viewing by unauthorized persons.

Where personal information is stored electronically or in databases, safeguards will ensure only authorized persons can access it.

When personal or financial information is no longer required, or once retention requirements have been met, it will be destroyed, erased, or anonymized securely. Paper documents containing names or identifying information will be destroyed by the Director of Operations using a third party service provider, Shred-IT.

Safeguards

Security safeguards protect personal information against loss, theft, and unauthorized access. Safeguards vary depending on the sensitivity of the information and may include:

- locked filing cabinets and secure storage for records not in use

- restricted access to the Director of Operations' files
- password-protected software used for collecting client information, statistical data, and volunteer schedules/information
- encryption in information systems
- up-to-date antivirus protection and routine backups
- computer firewalls
- timely, secure shredding of printed materials

When faxing or emailing personal information, staff will confirm the recipient is authorized and limit the information shared to what is necessary for its purpose.

Accessibility to Records
Clients and personnel may request access to their own records. In some cases, sufficient notice may be required and/or information may be withheld or redacted to protect the identity or personal information of others.

Privacy Breach Response
A privacy breach is when personal information is lost, stolen, accessed, used, or shared without permission.

If a breach is suspected or confirmed, staff and volunteers must:

1. Report it immediately to the Director of Operations.
2. Contain it (stop sharing, retrieve documents if possible, secure files/systems).
3. Document what happened (what info, who was involved, when/where it occurred).

The Director of Operations will:

4. Assess the risk and decide what actions are needed.
5. Notify the Chair of the Board, as appropriate, based on the seriousness of the breach and any lega, reputational, or safety risk.
6. Notify affected individuals and any required authorities as soon as reasonably possible.
7. Take steps to prevent it from happening again (training, process changes, security updates).

References and Related Documents

- Confidentiality Disclosure Agreement
- Ethical Code of Conduct
- Complaints Policy
- PIPEDA – The Personal Information Protection and Electronic Documents Act, 2000, last updated 03/04/2025
- A Guide for Individuals, Your Guide to PIPEDA

Reviewed and updated January 2026