

Privacy Policy and Protection of Personal Information

Adopted by the Board of Directors on June 18, 2024.

Introduction

The *Centre de Répit et Hébergement Maisons des Lucioles/Fireflies' Homes* is committed to protecting the privacy and confidentiality of personal information entrusted to it. We handle personal information in a responsible, ethical, and transparent manner and in accordance with applicable Canadian and Québec laws, including Québec's Act respecting the protection of personal information in the private sector (Law 25).

Designated Privacy Officer

The Executive Director acts as the Designated Privacy Officer and is responsible for overseeing the implementation of this policy, responding to questions, and handling requests related to personal information.

Principles

- Accountability for personal information.
- Collection limited to information necessary for identified purposes.
- No unauthorized disclosure of personal information.
- No discussion of confidential files with unauthorized persons.
- Appropriate security measures for personal information.
- Prompt reporting of confidentiality or security incidents.
- Respect for individuals' rights of access, correction, and deletion.

Collection and Use of Personal Information

We collect only the personal information necessary to provide services, manage participant, employee, donor, and partner records, organize activities, process donations, fulfill funding requirements, and comply with legal obligations.

- Name
- Postal address
- Email address
- Telephone number
- Date of birth
- Social Insurance Number (SIN), when required by law
- Medical information relevant to services provided
- Identification documents, when necessary

Personal information is collected directly from the individual whenever possible and is used only for the purposes for which it was collected.

Consent

Consent is obtained before collecting, using, or disclosing personal information, unless otherwise authorized or required by law. Individuals may withdraw consent at any time, subject to legal or contractual restrictions.

Data Retention and Destruction

Personal information is retained only as long as necessary for the purposes identified and is securely destroyed when no longer required.

Confidentiality

All board members, committee members, employees, volunteers, contractors, and suppliers must maintain the confidentiality of information obtained through their duties.

Disclosure of Personal Information

Personal information may be disclosed only with consent or when permitted or required by law, including to protect vital interests, comply with legal obligations, defend legal rights, or in connection with a merger or sale of the organization.

Security of Personal Information

- Physical and technical safeguards
- Access controls
- Data backup and recovery procedures
- Staff awareness and training
- Incident management procedures
- Confidentiality requirements for service providers

While we strive to protect personal information, no method of electronic transmission or storage is completely secure.

Access, Correction, and Updating

Individuals may request access to their personal information and request corrections by contacting the Designated Privacy Officer.

Cookies and Similar Technologies

Our website may use cookies and similar technologies to improve user experience, remember preferences, and analyze website usage.

Links to Other Websites

Our website may contain links to third-party websites. We are not responsible for their privacy practices.

Changes to This Policy

This policy may be updated from time to time. The most recent version will be posted on our website.

Contact Us

Centre de Répit et Hébergement Maisons des Lucioles
1805 Avenue de la Ronde
Québec, QC G1J 4E1
Phone: 418-527-6096 ext. 200
Email: direction@maisonsdeslucioles.ca

Conclusion

Maisons des Lucioles/Fireflies' Homes is committed to protecting personal information and ensuring that it is handled responsibly, securely, and in accordance with applicable privacy laws.

Appendix A – Data Security Incident Response Procedure

1. **Identification of the incident** – Employees and members must immediately report any suspected data security incident.
2. **Assessment and categorization** – Management assesses the seriousness of the incident and determines whether notification to authorities is required.
3. **Notification of external IT service provider** – Management informs the external IT provider and collaborates on the investigation.
4. **Containment and resolution** – Appropriate measures are taken to contain the incident and restore security.
5. **Communication and notification** – Affected individuals and authorities are informed when required by law.
6. **Analysis and prevention** – Root causes are analyzed and preventive measures are implemented.

7. **Policy and procedure updates** – Security policies and procedures are reviewed and updated following the incident.