Privacy and Data Protection Policy

Original endorsement date	**05/11/2024**
Date of current endorsement	**05/11/2024**
Summary	The policy outlines how the Pulse: South Metro Health Foundation collects, manages, and protects personal information, ensuring compliance with the Australian Privacy principles.
Review date	
Status	Active

Key definitions

Term	Definition
Personal Information	Information about an identified individual recorded in a material including names, addresses, email addresses, phone numbers, and financial details.
Sensitive Information	Information that is considered sensitive under the Privacy Act, such as racial or ethnic origin, political opinions, religious beliefs, health information, or sexual orientation.

Purpose

The purpose of this policy is to outline how the ***Pulse: South Metro Health Foundation*** (PSMHF) collects, manages, and protects personal information. The Foundation is committed to ensuring that the privacy and confidentiality of all personal data are respected and safeguarded in accordance with the **Australian Privacy Principles (APPs)** under the **Privacy Act 1988 (Cth)**. Additionally, this policy outlines the cybersecurity measures implemented to protect digital data and ensure personal information is secure.

1. Scope

This policy applies to all personal information collected, stored, used, and disclosed by the foundation. It includes the personal information of donors, employees, volunteers, and other stakeholders who interact with the foundation.

2. Collection of Personal Information

2.1 Types of Information Collected

The foundation may collect the following types of personal information:

- **Donor Information**: Name, contact details, donation history, and payment information.
- **Employee and Volunteer Information**: Employment or volunteer records, performance reviews, payroll details, and contact information.
- **Supporter Information**: Names, email addresses, and other contact details provided by individuals subscribing to newsletters or participating in events.

2.2 Purpose of Collection

The foundation will only collect personal information that is necessary for its operations, which include:

- Processing donations and providing tax receipts.
- Communicating with donors, employees, volunteers, and supporters.
- Administering fundraising campaigns and events.
- Meeting regulatory obligations.

2.3 Method of Collection

- Personal information will be collected directly from individuals, where possible, through forms, online submissions, emails, phone conversations, or event registrations.
- In some instances, personal information may be collected from third parties, such as publicly available sources or service providers, with the individual's consent or where permitted by law.

3. Use and Disclosure of Personal Information

3.1 Primary Use

- The foundation will only use personal information for the purpose for which it was collected or for which consent has been given, or for related purposes reasonably expected by the individual.
- This includes processing donations, communicating with donors, and providing information on the foundation's activities, campaigns, and events.

3.2 Disclosure to Third Parties

- Personal information may be disclosed to trusted third parties who provide services to the foundation, such as payment processors, mailing services, or IT support. These third parties are bound by confidentiality agreements and are required to comply with privacy standards equivalent to this policy.
- The foundation will not disclose or sell personal information to third parties for marketing purposes.
- Personal information will not be disclosed outside Australia.

3.3 Legal Requirements

- The Foundation may disclose personal information if required by law or to comply with regulatory obligations.

4. Data Security and Retention

4.1 Data Security

The foundation will take all reasonable steps to protect personal and foundation information from misuse, loss, unauthorised access, modification, or disclosure, by implementing the following **cybersecurity measures**:

- **Secure Servers**: Personal information stored digitally will be kept on secure servers with encryption protocols (e.g., SSL/TLS) in place to protect data during transmission.
- **Firewall and Intrusion Detection Systems**: Firewalls will be used to protect the foundation's internal network from external cyber threats. Additionally, intrusion detection and prevention systems will be implemented to monitor and block unauthorized access.
- **Access Controls and Authentication**: Strict access control policies will ensure that only authorised personnel have access to personal information. Multi-factor authentication (MFA) will be implemented for systems that store or process personal data to prevent unauthorised access.
- **Regular System Updates and Patching:** Regular updates and patching to all systems, software, and hardware are regularly updated and patched to protect against known vulnerabilities.
- **Data Encryption**: All sensitive and personal data stored digitally will be encrypted, both at rest (stored data) and in transit (during transmission), to prevent unauthorised access.
- **Regular Security Audits and Vulnerability Assessments**: Regular audits will be conducted to assess the effectiveness of cybersecurity protocols, and any vulnerabilities identified will be promptly addressed.
- **Anti-Malware and Antivirus Protection**: The foundation will maintain up-to-date anti-malware and antivirus software to detect, prevent, and respond to malicious attacks such as viruses, ransomware, and spyware.
- **Staff Training on Cybersecurity Awareness**: Staff will receive regular training on cybersecurity best practices, including how to recognise phishing attempts, suspicious attachments, and other cyber threats.

4.2 Cybersecurity Incident Response Plan

- The Foundation will maintain an updated **Cybersecurity Incident Response Plan** that outlines the procedures for responding to cyberattacks and data breaches. This plan will include roles and responsibilities, reporting protocols, and post-incident recovery actions.

4.3 Breach Notification

In the event of a **cybersecurity breach** where personal information is compromised (, the foundation will follow the steps outlined in the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988 (Cth) and take the following additional steps:

- **Immediate Containment**: The foundation will immediately implement measures to contain and mitigate further risks, such as isolating affected systems and resetting passwords.
- **Forensic Investigation**: A forensic investigation will be conducted to identify the cause of the breach, assess the extent of the damage, and determine whether additional information was compromised.
- **Incident Response Plan Activation:** The foundation will activate its Cybersecurity Incident Response Plan.
- **Reporting to Affected Parties**: The Foundation will notify affected individuals of the breach, explaining the nature of the incident and any steps they can take to protect themselves.
- **Notification to Regulatory Authorities**: The Foundation will notify the Office of the Australian Information Commissioner (OAIC) in accordance with NDB requirements if there is a risk of serious harm.

4.3 Retention of Personal Information

- The foundation will retain personal information for as long as necessary to fulfill the purposes for which it was collected, or as required by law.
- When personal information is no longer required, it will be securely destroyed or de-identified in accordance with applicable data retention policies. For digital information, secure methods such as data wiping or encryption-based destruction will be used to ensure that data cannot be recovered.

4.4 Secure Third-Party Integrations

- Where the Foundation uses third-party vendors or services for data processing, cloud storage, or IT services, strict security measures will be required of those vendors. Contracts with third-party vendors will include cybersecurity and privacy protection clauses that meet or exceed the Foundation’s internal standards.

5. Access and Correction of Personal Information

5.1 Right to Access

- Individuals have the right to request access to their personal information held by the Foundation. Requests can be made in writing to the foundation.
- Access will be granted unless there is a legal reason to deny the request, in which case the individual will be provided with an explanation.

5.2 Correction of Information

- Individuals have the right to request corrections to their personal information if they believe it is inaccurate, out of date, incomplete, or misleading.
- The foundation will promptly correct personal information upon receiving a request and verification of the updated information.

6. Anonymity and Pseudonymity

- Where it is lawful and practicable, individuals have the option to remain anonymous or use a pseudonym when interacting with the foundation, particularly in making donations or general inquiries.
- However, certain activities (such as issuing donation receipts) may require the provision of personal information.

7. Direct Marketing and Communication Preferences

7.1 Marketing Communications

The foundation may use personal information to communicate with individuals about its activities, fundraising campaigns, and events. All marketing communications will provide an option for recipients to opt out of future communications.

7.2 Opting Out

- Individuals can opt out of marketing communications at any time by using the “unsubscribe” feature in emails or by contacting the Foundation directly.
- Opting out of marketing communications will not affect the receipt of administrative communications (such as receipts for donations).

8. Complaints and Inquiries

8.1 Lodging a Complaint

If an individual believes the foundation has breached this policy or the Australian Privacy Principles, they may lodge a complaint in writing to the foundation.

8.2 Response to Complaints

The foundation will acknowledge receipt of the complaint within five business days and provide a written response within 30 business days of receiving the complaint. If more time is needed to resolve the issue, the complainant will be informed of the reason for the delay.

8.3 External Review

If an individual is dissatisfied with the Foundation's response to their complaint, they may refer the matter to the Office of the Australian Information Commissioner (OAIC) for further investigation.

10. Policy Review

This policy, including cybersecurity protocols, will be reviewed annually by the Board of Directors to ensure ongoing compliance with legal requirements and best practices in privacy, data protection, and cybersecurity. Updates to this policy will also reflect any new risks or technologies affecting the Foundation's cybersecurity posture.

11. Approval

Approved by the Directors on 05/11/2024.