Privacy Policy

1. Purpose and Objective

The Heart Foundation is committed to complying with all regulatory provisions related to privacy, as well as to maintaining and strengthening our reputation in the community.

This Policy sets out the Heart Foundation's position on how it deals with privacy-related compliance issues, including collection, use and disclosure of Personal Information and Sensitive Information. It outlines the systems in place that deal with privacy related complaints and actual or potential breaches of the Heart Foundation's legal obligations and procedures in regard to Personal Information handling practices.

2. Scope / Coverage

This internal Policy applies to all Heart Foundation Board members, honoraries, Staff, Contractors and Volunteers, and must be adhered to at all times.

3. Relevant Legislation and Related Documents

The primary legislation and regulatory provisions ("Key Regulatory Provisions") governing the Heart Foundation's privacy-related compliance obligations are:

- *Privacy Act 1988* (Cth)
- *Spam Act 2003* (Cth)
- *Do Not Call Register Act 2006* (Cth)
- Telecommunications (Telemarketing and Research Calls) Industry Standard 2017 (Cth)
- Part 6 of the *Telecommunications Act 1997* (Cth).
- Privacy Notice (the Heart Foundation's external facing APP privacy policy)
- Notifiable Data Breaches: Data Breach Response Plan
- Privacy Statements (as per the Heart Foundation's scripting document)

4. Definitions / Abbreviations

APP entity	An entity or organisation to which the Privacy Act applies.
Australian Privacy Principles	There are 13 APPs: 1. Open and transparent management of Personal Information 2. Anonymity and pseudonymity 3. Collection of solicited Personal Information 4. Dealing with unsolicited Personal Information 5. Notification of the collection of Personal Information 6. Use or disclosure of Personal Information 7. Direct marketing 8. Cross-border disclosure of Personal Information 9. Adoption, use or disclosure of government related identifiers 10. Quality of Personal Information 11. Security of Personal Information 12. Access to Personal Information 13. Correction of Personal Information
Consumers	Encompasses all individuals who come into contact with the Heart Foundation through any means, including but not limited to: a. The Heart Foundation Helpline b. Participating in heart health activities, events and fundraisers (e.g. Heart Foundation Walking or Jump Rope for Heart) c. Purchasing Heart Foundation merchandise d. Donating, or being invited to donate, to the Heart Foundation e. Participating in or donating to fundraising activities f. Making a request for information or contact g. Applying for (and/or receiving) Heart Foundation Research Program grants;

	h. Professionals accessing Heart Foundation resources in their professional capacity (e.g. Cardiologists, school teachers in relation to Jump Rope for Heart) i. Any other means where Personal Information may be collected about an individual.
Contractors	Persons engaged on a contractual or sub-contractual basis to provide services to the Heart Foundation. This includes web-based service providers.
Data Breach Response Plan	Sets out the procedure around how the Heart Foundation will respond in the event of a Notifiable Data Breach (as defined by the Australian *Privacy Act 1988*). This Data Breach Response Plan can be found in the Library on *Red*.
Do Not Call Register Act (DNCR Act)	This Act prohibits unsolicited telephone calls or facsimile transmissions to numbers listed on the Do Not Call Register.
Legal Team	The Heart Foundation's in-house Legal Team. The Legal Team can be contacted at legal@heartfoundation.org.au.
Part 6 of the *Telecommunications Act* (Cth)	Part 6 of the Act mandates that all telemarketing and fax marketing agreements should contain an express provision requiring compliance with industry codes and standards.
Personal Information	As defined under the *Privacy Act 1988* (Cth), Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not. Examples of Personal Information include name, address, date of birth, email address, telephone number, bank account and financial details. Personal Information may include Sensitive Information (see below).
Privacy Act	This Act protects the handling of Personal and Sensitive information about individuals. This includes the collection, use, storage and disclosure of Personal Information.
Privacy Induction	The Privacy Induction training program is regularly provided by the Legal Team across the business
Privacy Notice	The public-facing Privacy Notice (sometimes referred to as the "Privacy Policy") that appears at www.heartfoundation.org.au.
Privacy Policy	This internal document.
Privacy Refresher	The Privacy Refresher training program is regularly provided by the Legal Team.
Privacy Statement	The scripted wording that accompanies any collection of Personal Information. Approved Heart Foundation Privacy

	Statements and guidance for use can be found on Red. Privacy Statements must be used in accordance with the guidance provided in the Privacy Statement scripting document to ensure that the collection notice is brought to the attention of the individual. This is also important to ensure that the collection notice can be relied on to constitute inferred consent pursuant to key regulatory provisions (e.g. the *Spam Act* and the *DNCR Act*)
Sensitive Information	Under the *Privacy Act*, Sensitive Information means: a. information or an opinion about an individual's: i. racial or ethnic origin; or ii. political opinions; or iii. membership of a political association; or iv. religious beliefs or affiliations; or v. philosophical beliefs; or vi. membership of a professional or trade association; vii. membership of a trade union; or viii. sexual preferences or practices; or ix. criminal record; that is also personal information; or b. health information about an individual; or c. genetic information about an individual that is not otherwise health information; or d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or e. biometric templates. For the purposes of this document, Sensitive Information also includes credit card information.
Spam Act	The Spam Act prohibits the sending of unsolicited commercial electronic messages. The Spam Act covers email, instant messaging, SMS and MMS (text and image-based mobile phone messaging) of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing.
Specified Role	Privacy Induction and Privacy Refresher training is considered mandatory for persons occupying Specified Roles: All members of the following teams:

	• Office of the CEO, Executive Team and Leadership Team; • All Heart Health teams; • Advocacy, Government Relations & Public Policy • Development Group; • Marketing, Media & Communications; • Strategy, Renewal and Performance • Legal; • People and Culture; • Finance & Office Services; In addition: • all other staff whose role involves acquiring, managing or using Personal Information; • all office volunteers whose role involves acquiring, managing or using Personal Information; and • all other staff or categories of staff nominated by the Heart Foundation's General Counsel from time to time. All staff are encouraged to participate in Privacy Induction and Refresher training; however, it is not mandatory unless they are included in the abovementioned categories
Staff	Includes the Board members, honoraries, Executive Officers, Managers, Supervisors, employees and Volunteers unless otherwise indicated or implied.
Telecommunications (Telemarketing and Research Calls) Industry Standard 2017)	This Standard relates to telemarketing and research calls and establishes a minimum set of requirements: restricting the calling hours/days for making telemarketing and research calls; requiring provision of specific information by the caller; providing for the termination of calls; and requiring callers to enable calling line identification.
Volunteers	Unpaid volunteers who offer their time and skills to the Heart Foundation including, but not limited to: walk organisers, event volunteers, community speakers, and administration support volunteers.

5. Policy

5.1 *Privacy Policy*

In order to uphold its ethical and reputational values, the Heart Foundation seeks to go beyond merely meeting the minimum regulatory requirements in protecting the personal information we hold. Rather, we strive to exceed regulatory requirements and meet the expectations of our supporters and industry best practice.

The Heart Foundation is committed to upholding all 13 Australian Privacy Principles (APPs) enacted under the Privacy Act which provide guidance as to how Personal and Sensitive Information should be managed.

The Heart Foundation acknowledges that it is an APP entity, meaning that it is a private sector organisation with an annual turnover of more than $3 million, and as a consequence the APPs apply to the organisation as a whole.

As an APP entity, the Heart Foundation is required to comply with the Notifiable Data Breaches Scheme effective 22 February 2018. The Heart Foundation's Notifiable Data Breaches: Data Breach Response Plan, which is available in the Library on Red, provides more detail on how the Heart Foundation will respond in the event that a Notifiable Data Breach occurs.

The Heart Foundation takes its responsibilities under the Privacy Act seriously and will dedicate resources to ensure compliance with all aspects of the APPs as they relate to the Heart Foundation's operations.

The Heart Foundation's Privacy Notice serves as the Heart Foundation's externally facing "Privacy Policy" and can be found at www.heartfoundation.org.au. It informs individuals about the management of their Personal Information by the Heart Foundation. Further, more detailed information is provided to individuals at the point that their Personal Information is collected. This collection notice is contained in the Heart Foundation's approved scripted Privacy Statement document. Internally, Staff obligations with respect to privacy-related regulatory compliance are detailed in the Privacy Policy (this document).

5.2 *Australian Privacy Principles*

The Heart Foundation's position regarding the Australian Privacy Principles (APPs) is as follows:

5.2.1 *APP 1 – Open and transparent management of personal information*

Scope: Ensures that APP entities manage Personal Information in an open and transparent way. This includes having a clear and up-to-date Privacy Policy.

Position: The Heart Foundation is open and honest regarding its position on privacy and publishes a public Privacy Notice on the Heart Foundation's website. A link to the Privacy Notice is included in all relevant publications and in Heart Foundation approved Privacy Statements, which must be used wherever Personal Information is collected. This includes, for example in registration forms and surveys. The Privacy Notice covers the required information listed in APP 1.4.

The Heart Foundation will take all reasonable steps to ensure that the APP's are complied with and that all inquiries or complaints from individuals regarding such compliance are promptly addressed.

5.2.2 *APP 2 – Anonymity and pseudonymity*

Scope: Requires APP entities to give individuals the option of not identifying themselves, or using a pseudonym. Limited exceptions apply.

Position: Wherever it is lawful and practical, the Heart Foundation will allow people to use a pseudonym or interact anonymously (e.g. when browsing the Heart Foundation's public website).

5.2.3 *APP 3 – Collection of solicited Personal Information*

Scope: Outlines when an APP entity can collect Personal Information that is solicited. It applies higher standards to the collection of Sensitive Information.

Position: The Heart Foundation will only collect Personal Information (including Sensitive Information) where it is required to effectively perform a function, and will collect it in a fair, lawful and unobtrusive manner. An approved Heart Foundation Privacy Statement must be used whenever Personal Information is collected.

Approved Heart Foundation Privacy Statements can be found in the Privacy Statement Scripting document in the Library on Red. In using approved Privacy Statements Staff must adhere to the guidance notes set out in the scripting document.

All records of Personal Information must include the following information:

1. The date on which the Personal Information was acquired;

2. The source from which the Personal Information was acquired; and
3. Details of the consent given.

Where Personal Information is obtained from a third party (e.g. rented/purchased/shared lists or via a third-party application or platform), the agreement for acquisition of the data must be referred to the Legal Team to ensure that appropriate privacy provisions are included in the agreement and to ensure due diligence is undertaken to ascertain whether the list provider is able to evidence that appropriate consent has been obtained from those whose data is contained on the list.

Where Personal Information is to be used by or disclosed to any third party or contracted service provider, the relevant agreement must be referred to the Legal Team to ensure that appropriate privacy provisions are included in the agreement.

In addition, the Heart Foundation Staff member responsible for referring the matter to the Legal Team will obtain a statement from the third party confirming it abides by the Privacy Act in collecting, using and disclosing information and detailing the basis upon which that party has consent to share the information with the Heart Foundation for the purpose intended.

The Heart Foundation will not collect Sensitive Information (see "Definitions" below) unless it is required to, to carry out one of its main functions. Any collection of Sensitive Information will be carried out with the person's permission, and a record of that permission will be held

5.2.4 *APP 4 — Dealing with unsolicited Personal Information*

Scope: Outlines how APP entities must deal with unsolicited Personal Information.

Position: If the Heart Foundation receives Personal Information which it did not solicit it will promptly determine whether it would have been permitted to collect that information under APP 3. If the Heart Foundation would have been permitted to collect the information, it will be treated as solicited Personal Information. If the Heart Foundation is not permitted to collect the unsolicited information it will take steps to ensure that the information is destroyed or de-identified as soon as is practicable.

5.2.5 *APP 5 — Notification of the collection of Personal Information*

Scope: Outlines when and in what circumstances an APP entity that collects Personal Information must notify an individual of certain matters. Those matters are specified in subclause 5.2 of APP 5.

Position: The Heart Foundation will provide notice of collection to individuals before or at the time that their Personal Information is collected or, if that is not practicable, then as soon as possible afterwards. The notice is contained in the Heart Foundation's approved Privacy Statements, and must be used wherever Personal Information is collected. Privacy Statements must be used in accordance with the guidance provided in the Privacy Statement scripting document to ensure that the Privacy Notice is brought to the attention of the individual. This is also important to ensure that the Privacy Notice can be relied on to constitute inferred consent pursuant to other Key Regulatory Provisions (e.g. the Spam Act and the DNCR Act).

5.2.6 *APP 6 — Use or disclosure of Personal Information*

Scope: Outlines the circumstances in which an APP entity may use or disclose Personal Information that it holds.

Position: The Heart Foundation will only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose of collection.

Personal Information may also be disclosed (without consent) in limited circumstances, where required by law, such as to assist with law enforcement or in the event of serious threats to life, health or safety.

The Heart Foundation will not sell, swap, or share Personal Information with any other party except where that party is providing services to the Heart Foundation and those services are subject to an agreement which has been approved by the Legal team and contains all relevant privacy-related provisions. The collection notice provided in the Heart Foundation's approved Privacy Statements makes this point clear to reassure those who may be concerned about passing on their information to the Heart Foundation. Where data is made available to contracted service providers it is to be made available only for the provision of the contracted service and may not be used for any other purpose.

5.2.7 *APP 7 — Direct marketing*

Scope: An organisation may only use or disclose Personal Information for direct marketing purposes if certain conditions are met.

Position: The Heart Foundation will provide guidance to Staff regarding the use of Personal Information for direct marketing purposes and that guidance will reflect the conditions specified in APP 7.

Staff must ensure that if a consumer requests that no further direct marketing communications be sent to them, that these requests get passed on to any relevant service provider. These consumers should also be added to the Heart Foundation's internal Do Not Contact Register as soon as is reasonably practicable. These requests must be actioned within five business days.

5.2.8 *APP 8 — Cross-border disclosure of Personal Information*

Scope: Outlines the steps an APP entity must take to protect Personal Information before it is disclosed overseas.

Position: In the event consideration is given to disclosing, and/or transferring Personal Information to a foreign recipient, the Heart Foundation will ensure all requirements & safeguards required by the Privacy Act are met and the Heart Foundation will take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs.

5.2.9 *APP 9 — Adoption, use or disclosure of government related identifiers*

Scope: Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Position: The Heart Foundation uses a system of donor numbers to identify individual database records. These donor numbers are not related to government agency identifiers such as tax file numbers or Medicare numbers. The Heart Foundation will not use government related identifiers unless it complies with one of the limited circumstances specified in the Act.

5.2.10 *APP 10 — Quality of Personal Information*

Scope: An APP entity must take reasonable steps to ensure the Personal Information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the Personal Information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

Position: The Heart Foundation will take all reasonable steps to ensure the Personal Information it collects, uses or discloses is accurate, complete, relevant and up to date having regard to the purpose of the collection, use or disclosure.

5.2.11 *APP 11 — Security of Personal Information*

Scope: An APP entity must take reasonable steps to protect Personal Information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify Personal Information in certain circumstances.

Position: The Heart Foundation will ensure the security of all information it collects through various means, including, but not limited to:

1. Physical security of its premises;
2. Taking reasonable steps to confirm the identify of persons wishing to access Personal Information;
3. IT security, including password protection, security level access and role-based permissions to Personal Information, and encryption of data transmissions where prudent; and
4. Training Staff on information security.

5.2.12 *APP 12 — Access to Personal Information*

Scope: Outlines an APP entity's obligations where an individual has requested access to their Personal Information. This includes a requirement to provide access unless a specific exception applies.

Position: All requests for access to Personal Information will be dealt with promptly and courteously by Heart Foundation Staff. Requests will be immediately directed to the Privacy Officer for actioning.

5.2.13 *APP 13 — Correction of Personal Information*

Scope: Outlines an APP entity's obligations in relation to correcting the Personal Information it holds about individuals.

Position: All requests for correction of Personal Information will be dealt with promptly and courteously by Heart Foundation Staff. Requests will be immediately directed to the Privacy Officer for actioning.

5.3 *Compliance with other privacy-related Key Regulatory Provisions*

The Heart Foundation requirements for compliance with other privacy-related Key Regulatory Provisions are detailed in the Privacy-Related Policies and procedures, as

updated from time to time. The Privacy-Related Policies and procedures are located in the Library on *Red.*

6. Roles and Responsibilities

This policy applies to all Board members, honoraries, Staff, Contractors and Volunteers, and must be adhered to at all times Responsibility for complying with the Heart Foundation's privacy-related compliance obligations rests with everyone.

Role: Board	
Responsibility	**Frequency**
Ensures that the Policy is in place and is reviewed.	Ongoing
Oversee, review and approve this Policy.	Every two years
Remain abreast of the Heart Foundation's obligations under the Key Regulatory Provisions, and the provision of high level direction to the Heart Foundation regarding the Heart Foundation's position on privacy-related compliance, including the resolution of actual or potential breaches of privacy-related policies, procedures, complaints and training.	Ongoing
Review any escalated privacy queries, complaints and issues, including any contact from regulators or lawyers as referred by the Risk, Audit & Governance Committee.	As required
Monitor compliance with privacy-related policies and procedures and escalating any breaches referred by the Risk, Audit & Governance Committee.	As required
Role: Risk, Audit and Governance Committee (RAG Committee)	
Responsibility	**Frequency**
Endorse this Policy.	Every two years
Review any escalated privacy queries, complaints and issues, including any contact from regulators or lawyers for referral to the Board and liaising with the relevant Local Privacy Officer to manage and finalise any matters.	As required
Monitor compliance with privacy-related policies and procedures and escalating any breaches for referral to the Board.	As required
Role: Group CEO	
Responsibility	**Frequency**
Ensures that the Heart Foundation develops procedures and controls to implement the policy.	Ongoing

Be fully aware of the Heart Foundation's obligations under the Key Regulatory Provisions.	Ongoing
Ensure all Staff are familiar with the Heart Foundation's privacy-related policies and procedures.	Ongoing
Ensure all Staff have access to effective and appropriate privacy-related compliance training.	Ongoing
That all Heart Foundation websites include a link to the current public Privacy Notice found on the public Heart Foundation website www.heartfoundation.org.au.	Ongoing
Ensure they comply with all responsibilities outlined under People Leaders and All Staff.	Ongoing
Role: Executive Group	
Responsibility	**Frequency**
Oversee, review and endorses this Policy	Every two years
Remain abreast of the Heart Foundation's obligations under the Key Regulatory Provisions, and the provision of high-level direction to the Board regarding the Heart Foundation's position on privacy-related compliance (including actual or potential breaches, complaints and training).	Ongoing
Ensure they comply with all responsibilities outlined under People Leaders and All Staff.	Ongoing
Role: General Counsel	
Responsibility	**Frequency**
Remain up to date regarding changes to the Key Regulatory Provisions and any impact these changes may have on the Heart Foundation's privacy-related compliance obligations and privacy-related policies and procedures. This includes monitoring changes in both Commonwealth and State/Territory requirements.	Ongoing
Provide training materials for use in the Privacy Induction and Privacy Refresher programs and any bespoke training as required.	Ongoing
Develop and maintain privacy-related policies and procedures with the assistance of Local Privacy Officers and facilitate implementation throughout the Heart Foundation.	Ongoing
Audit and administer reviews of the Heart Foundation's compliance with privacy-related policies and procedures.	Ongoing
Oversight of the privacy mailbox at privacy@heartfoundation.org.au and ensuring that where necessary, emails are forwarded to Supporter Relations or the appropriate Staff member for action.	Ongoing

Take phone calls where a call is received asking to speak to the Privacy Officer and managing queries, complaints and issues that may arise from such calls.	As required
Receive and manage emails and letters regarding privacy queries, complaints and issues from both Staff and members of the public.	Ongoing
Manage actual, suspected or potential data breaches in accordance with the Data Breach Response Plan.	Ongoing
Maintain accurate records regarding access/correction requests and complaints.	Ongoing
Prepare and submit for sign-off, of all privacy-related policies and any amendments to those documents.	Ongoing
Refer escalated privacy queries, complaints and issues, including any contact from regulators or lawyers to the Risk, Audit & Governance Committee for referral to the Board and liaising with the relevant Local Privacy Officer to manage and finalise any matters.	As required
Monitor compliance with privacy-related policies and procedures and escalating any breaches to the Risk, Audit & Governance Committee for referral to the Board.	Ongoing
Role: People Leaders	
Responsibility	**Frequency**
Ensure staff, volunteers and themselves are aware of and comply with this Policy.	Ongoing
Ensure they are fully aware of the Heart Foundation's obligations under the Key Regulatory Provisions.	Ongoing
Provide appropriate leadership & direction to ensure the Heart Foundation's privacy-related policies and procedures are effectively implemented in their area of responsibility.	Ongoing
Monitor the quality and effectiveness of the management and use of Personal Information, and taking appropriate action (in consultation with the National Privacy Officer) to address any risks, gaps or shortcomings.	Ongoing
Ensure that all Staff occupying Specified Roles complete Privacy Induction within six weeks of commencement with the Heart Foundation.	Ongoing
Ensure that all Staff occupying Specified Roles complete the annual Privacy Refresher training.	Ongoing
Ensure Staff whose scope of work includes privacy-related compliance obligations have the information, skills, support and training they need to effectively comply with the Heart Foundation's privacy-related policies and procedures; Including privacy-related compliance	Ongoing

provisions in policies, procedures, contracts and business plans where appropriate.	
Refer any privacy-related agreements to the Legal Team for review prior to commencement or execution of the contract.	Ongoing
Report all privacy-related complaints, breaches, or potential breaches of privacy related policies or procedures to the National Privacy Officer.	Ongoing
Ensure they comply with all responsibilities outlined under All Staff.	Ongoing
Role: All Staff	
Responsibility	**Frequency**
Comply with the policy	Ongoing
Ensure they are fully aware of the Heart Foundation's obligations under the Key Regulatory Provisions as they pertain to their role.	Ongoing
Comply with all privacy-related policies and procedures relevant to their role.	Ongoing
Refer any privacy-related agreements to the Legal Team for review prior to commencement or execution of the contract	Ongoing
Report any privacy-related complaints, breaches, or potential breaches, of privacy-related policies or procedures to their supervisor or manager.	Ongoing
Report to their manager, the Legal team and Chief Information Officer any actual, suspected or potential data breaches as detailed in the Data Breach Response Plan	As required
Complete the Privacy Induction training program within six weeks of commencing their role, if their role is a Specified Role.	Ongoing
Complete the Privacy Refresher training program annually, if their role is a Specified Role.	Ongoing

7. Review and Document Control

The policy is to be reviewed every two years or as determined by the Board.

Policy Type	Governance Policy	
Function Owner	Legal	
Version Number	5.0	
Approved Date	31/08/2020	
Endorsement Dates	**Executive Group**	**RAGC**
	18/02/2020	16/04/2020
Scheduled Review Date	31/08/2022	

8. Attachments

Nil