

The Reframe Foundation Ltd

Privacy Policy

1. Statement of Commitment

1.1 Commitment to Privacy

The Reframe Foundation Ltd [ACN 691 498 692](#) ("Reframe") is committed to protecting the privacy, dignity, autonomy and safety of every individual who engages with the organisation.

Privacy is fundamental to the trust placed in Reframe by victim-survivors of domestic and family violence, children and young people, donors, volunteers, employees, contractors, lived experience contributors and members of the broader community.

Reframe recognises that the inappropriate collection, use or disclosure of personal information may expose individuals to significant physical, psychological, social or financial harm. Accordingly, the organisation is committed to maintaining a privacy management framework that reflects Australian law, contemporary governance standards and trauma-informed practice.

1.2 Privacy as a Governance Responsibility

Reframe recognises that protecting personal information is not solely a legislative obligation but a core governance responsibility. Effective privacy management supports the organisation's charitable purpose, protects the rights of individuals, promotes public confidence and contributes to the safe delivery of services.

The Board of Directors is responsible for overseeing the organisation's privacy governance framework and ensuring that appropriate systems, resources and oversight mechanisms are in place to support compliance with applicable legislation.

2. Commitment to Trauma-Informed Practice

As a domestic and family violence organisation, Reframe acknowledges that many individuals who engage with the organisation have experienced trauma, coercive control, abuse or violence. Privacy practices must therefore extend beyond legal compliance and actively contribute to the safety and wellbeing of those individuals.

Decisions relating to the collection, use, disclosure and storage of personal information will be informed by the principles of trauma-informed practice, recognising the importance of safety, trust, collaboration, empowerment and respect.

Where privacy considerations and individual safety intersect, Reframe will adopt a risk-based approach that seeks to minimise the possibility of further harm while complying with applicable legal obligations.

2. Purpose

2.1 Purpose of this Policy

The purpose of this Policy is to establish the governance principles that guide the collection, management, use, disclosure, storage, retention and disposal of personal information by Reframe. The Policy provides a consistent framework for protecting personal information throughout its lifecycle and demonstrates the organisation's commitment to meeting its obligations under Australian privacy legislation.

2.2 Objectives

The objectives of this Policy are to:

- a. ensure personal information is collected, used and disclosed lawfully, fairly and transparently;
- b. protect the privacy, dignity and safety of individuals who engage with Reframe;
- c. establish clear governance responsibilities for privacy management across the organisation;
- d. support compliance with the *Privacy Act 1988 (Cth)*, the Australian Privacy Principles (APPs) and other applicable legislation;
- e. promote accountability, transparency and continuous improvement in privacy practices; and
- f. strengthen public confidence in Reframe's ability to responsibly manage personal information.

This Policy should be read together with any other organisational policies governing the management of information.

3. Scope

3.1 Application

This Policy applies to all personal information handled by Reframe, irrespective of the format in which the information is held or the manner in which it is collected. It applies to information stored electronically, in paper records, audio or visual recordings, cloud-based systems, email correspondence, messaging platforms and any other medium through which personal information is created, received or maintained.

3.2 Persons Covered

This Policy applies to all persons acting on behalf of Reframe, including:

- a. members of the Board of Directors;
- b. employees, whether permanent, temporary or casual;
- c. volunteers;
- d. contractors and consultants;
- e. students and work experience participants;
- f. agency personnel; and
- g. any third party authorised to collect, access or manage personal information on behalf of Reframe.

All persons covered by this Policy are required to comply with its requirements and any associated organisational procedures.

3.3 Information Covered

This Policy applies to all personal information collected or managed by Reframe in connection with its activities, including information relating to:

- a. victim-survivors of domestic and family violence;
- b. children and young people;
- c. donors and supporters;
- d. volunteers and prospective volunteers;
- e. employees and prospective employees;
- f. contractors and consultants;
- g. Board members;
- h. lived experience contributors;
- i. researchers, partners and stakeholders; and
- j. any other individual who engages with the organisation.

Where information constitutes sensitive information under the *Privacy Act 1988 (Cth)*, additional protections described in this Policy apply.

4. Legislative Framework

4.1 Legislative Context

The Reframe Foundation Ltd is committed to complying with all applicable privacy, information management and safeguarding legislation relevant to its operations. This Policy has been developed primarily to support compliance with the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles (APPs), while recognising that Reframe may also be subject to additional Commonwealth, State and Territory legislation depending on the nature of its activities, funding arrangements and service delivery.

Privacy obligations are not limited to legislative compliance. Reframe acknowledges that contemporary privacy governance requires the organisation to adopt systems, practices and organisational culture that actively protect personal information, support transparency and accountability, and minimise the risk of harm arising from inappropriate information handling.

4.2 Primary Legislation

This Policy is primarily informed by the following legislation, as amended from time to time:

- a. *Privacy Act 1988 (Cth)*;
- b. the Australian Privacy Principles contained in Schedule 1 of the *Privacy Act 1988 (Cth)*;
- c. the *Privacy and Other Legislation Amendment Act 2024 (Cth)*, to the extent applicable;
- d. the Notifiable Data Breaches Scheme established under Part IIIC of the *Privacy Act 1988 (Cth)*;
- e. the *Australian Charities and Not-for-profits Commission Act 2012 (Cth)*;
- f. applicable Commonwealth, State and Territory child protection legislation;
- g. records management legislation applicable to jurisdictions in which Reframe operates; and
- h. any other legislation governing the lawful collection, use, disclosure or storage of personal information.

Where legislative obligations are inconsistent, Reframe will seek legal advice and comply with the requirements that most appropriately protect the rights and safety of affected individuals, unless otherwise required by law.

4.3 Australian Privacy Principles

The Australian Privacy Principles establish the minimum standards for the handling of personal information by organisations subject to the *Privacy Act 1988 (Cth)*.

Reframe's privacy management framework has been developed to support compliance with each of the Australian Privacy Principles, including:

- **APP 1** – Open and transparent management of personal information.
- **APP 3** – Collection of solicited personal information.
- **APP 5** – Notification of the collection of personal information.
- **APP 6** – Use and disclosure of personal information.
- **APP 10** – Quality of personal information.
- **APP 11** – Security of personal information.
- **APP 12** – Access to personal information.
- **APP 13** – Correction of personal information.

Compliance with these principles is achieved through this Policy, supporting organisational procedures, staff training, governance oversight and continuous improvement.

4.4 Other Legal Obligations

Reframe recognises that circumstances may arise where legislation authorises or requires the collection, use or disclosure of personal information without an individual's consent. These circumstances may include mandatory reporting obligations, compliance with court orders, lawful requests from regulatory authorities, safeguarding responsibilities, or circumstances involving a serious threat to the life, health or safety of an individual.

Where such obligations arise, Reframe will ensure that any disclosure is limited to the information reasonably necessary to satisfy the relevant legal requirement and that appropriate records of the disclosure are maintained.

4.5 Standards and Guidance

In addition to legislative requirements, Reframe is committed to aligning its privacy practices with recognised Australian guidance and contemporary governance standards. This includes guidance published by the Office of the Australian Information Commissioner (OAIC), best practice recommendations relating to privacy governance, information security and data breach response, and trauma-informed approaches to managing personal information within community services.

5. Definitions

The following definitions apply for the purposes of this Policy. Unless otherwise stated, words and expressions used in this Policy have the same meaning as under the *Privacy Act 1988 (Cth)*.

Australian Privacy Principles or APPs means the principles contained in Schedule 1 of the *Privacy Act 1988 (Cth)* that regulate the collection, use, disclosure, storage and management of personal information by organisations.

A **Child** means a person under the age of 18 years.

Consent means a voluntary, informed, current and specific agreement by an individual to the collection, use or disclosure of their personal information. Consent may be express or implied where permitted by law; however, Reframe will seek express consent wherever practicable when collecting or using sensitive information.

De-identified Information means information that has been altered or managed so that an individual is no longer reasonably identifiable. Reframe acknowledges that de-identification is an ongoing process and will take reasonable steps to minimise the risk of re-identification.

Health Information has the meaning given under the *Privacy Act 1988 (Cth)* and includes information or opinions about an individual's physical or mental health, disability, health services received or health status.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether it is recorded in a material form or otherwise.

The **Privacy Officer** is the person appointed by Reframe to oversee the organisation's privacy management framework, provide advice regarding privacy compliance, coordinate responses to privacy incidents and complaints, monitor legislative developments and support continuous improvement in privacy governance.

Sensitive Information has the meaning given under the *Privacy Act 1988 (Cth)* and includes information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, criminal record, biometric information, genetic information and health information.

For Reframe, Sensitive Information also commonly includes information concerning domestic and family violence, safety planning, risk assessments, counselling, safeguarding concerns and information relating to children. While not all of this information is technically classified as "sensitive information" under the *Privacy Act*, Reframe will manage it with an equivalent level of protection because of the significant risk that inappropriate disclosure could pose to individuals.

Trauma-Informed Practice means an approach to service delivery and information management that recognises the prevalence and impacts of trauma, prioritises physical and emotional safety, promotes trust, respects individual autonomy, supports collaboration and seeks to avoid practices that may re-traumatise individuals.

A **Victim-Survivor** means a person who has experienced domestic, family or sexual violence or other forms of interpersonal violence, recognising that individuals may identify differently and that respectful language should always be used in accordance with their preferences.

6. Privacy Governance Principles

6.1 Purpose

Privacy governance at The Reframe Foundation Ltd is founded on the principle that the respectful management of personal information is essential to maintaining trust, protecting individual rights and delivering safe, ethical and effective services. Every person acting on behalf of Reframe shares responsibility for ensuring that personal information is handled lawfully, securely and with appropriate regard for the dignity and safety of the individuals concerned.

The following principles guide all decisions relating to the management of personal information and are intended to complement, rather than replace, the specific requirements contained within the *Privacy Act 1988 (Cth)* and other applicable legislation.

6.2 Respect for Privacy and Human Dignity

Reframe recognises privacy as a fundamental human right and an essential component of personal dignity, autonomy and wellbeing. Individuals who engage with the organisation must be able to do so with confidence that their personal information will be handled respectfully and responsibly.

Privacy extends beyond legal compliance. It includes recognising an individual's right to determine how their personal information is collected, used and shared, and acknowledging that the inappropriate handling of personal information can undermine trust, compromise safety and cause significant emotional or psychological harm.

All decisions involving personal information should therefore be made with consideration for the individual's dignity, personal circumstances and reasonable expectations.

6.3 Trauma-Informed Privacy Practice

Reframe adopts a trauma-informed approach to privacy management. The organisation acknowledges that many individuals engaging with its services have experienced domestic and family violence, coercive control, abuse, exploitation or other traumatic events.

Privacy practices must therefore actively contribute to an individual's physical and emotional safety. Before collecting, using or disclosing personal information, personnel must consider whether the proposed action could unintentionally expose an individual to further harm, compromise an existing safety plan or reduce the individual's willingness to seek support.

Trauma-informed privacy practice requires personnel to communicate respectfully, provide clear explanations regarding information handling, avoid unnecessary requests for personal information and ensure that individuals understand the choices available to them wherever practicable.

Where there is uncertainty regarding the safest approach to managing information, the organisation will adopt a precautionary approach that prioritises the safety and wellbeing of affected individuals while remaining consistent with legal obligations.

6.4 Privacy by Design and by Default

Reframe is committed to embedding privacy considerations into organisational governance, decision-making and service design from the earliest stages of planning.

Whenever new programs, technologies, partnerships, digital platforms, fundraising initiatives, research projects or administrative processes are introduced, privacy risks should be considered before implementation rather than after problems arise.

The organisation will seek to ensure that systems and processes are designed so that privacy protections are incorporated as a default setting. Wherever reasonably practicable, only the minimum personal information necessary for the relevant activity will be collected, access to information will be appropriately restricted and appropriate security measures will be incorporated into organisational systems.

Where a proposed initiative is likely to involve significant privacy risks, Reframe should undertake a Privacy Impact Assessment before implementation to identify potential risks and appropriate mitigation strategies.

6.5 Data Minimisation

Reframe is committed to collecting, using and retaining only the personal information that is reasonably necessary to achieve a legitimate organisational purpose.

Personnel must not request information simply because it may be useful in the future or because it has historically been collected. Before collecting information, consideration should be given to whether the relevant purpose can be achieved using less information, de-identified information or information that is already held by the organisation.

Similarly, where personal information is disclosed, only the minimum amount of information necessary to achieve the intended purpose should be shared.

Applying the principle of data minimisation reduces privacy risks, strengthens information security and supports compliance with the Australian Privacy Principles.

6.6 Purpose Limitation

Personal information entrusted to Reframe will only be used or disclosed for the purpose for which it was collected, for a directly related purpose that an individual would reasonably expect, or where otherwise authorised or required by law.

The organisation will not use personal information for purposes that are incompatible with its charitable mission or inconsistent with the reasonable expectations of the individual concerned.

Where Reframe proposes to use personal information for a substantially different purpose, the organisation will obtain the individual's consent unless another lawful basis for the proposed use applies.

6.7 Confidentiality

Confidentiality is fundamental to maintaining trust with victim-survivors, children, employees, volunteers, donors and the wider community.

All persons acting on behalf of Reframe are required to maintain the confidentiality of personal information obtained through their work with the organisation. Confidential information must not be discussed with persons who do not have a legitimate need to know the information and must never be accessed out of curiosity or for personal purposes.

The obligation of confidentiality continues after an individual's employment, volunteer engagement or contractual relationship with Reframe has ended.

Reframe does not sell, rent, trade or otherwise commercially exploit personal information.

6.8 Accountability

Privacy protection is a shared organisational responsibility.

The Board of Directors, Chief Executive Officer, Privacy Officer, managers, employees, volunteers and contractors each play an important role in ensuring that personal information is managed appropriately.

Individuals are expected to understand their privacy obligations, complete relevant training, report suspected privacy incidents promptly and cooperate with organisational efforts to strengthen privacy governance.

Where privacy obligations are not met, Reframe will take appropriate action consistent with its policies, contractual arrangements and applicable legislation.

6.9 Continuous Improvement

Privacy governance is an ongoing process rather than a single compliance activity.

Reframe is committed to regularly reviewing its privacy framework to ensure that it remains effective, legally compliant and responsive to emerging risks, technological developments and changes in community expectations.

The organisation will periodically review its policies, procedures, training programs, information security measures, incident response processes and governance arrangements to identify opportunities for improvement. Lessons learned from privacy incidents, complaints, audits and stakeholder feedback will be incorporated into future policy and operational improvements wherever appropriate.

7. Collection of Personal Information

7.1 Commitment to Responsible Collection

The Reframe Foundation Ltd is committed to collecting personal information lawfully, fairly and respectfully. Personal information will only be collected where it is reasonably necessary for Reframe to perform its charitable functions, deliver services, meet legal obligations, administer its operations or undertake activities directly related to its purpose.

As a domestic and family violence organisation, Reframe recognises that individuals may disclose highly sensitive personal information while experiencing trauma, crisis or significant vulnerability. The organisation will therefore only collect the personal information that is reasonably necessary to understand an individual's circumstances, provide appropriate services or fulfil an identified legal, contractual or operational purpose.

Individuals will not be required to provide information that is unnecessary for the services requested or the functions being performed.

7.2 Lawful and Fair Collection

Reframe will collect personal information by lawful and fair means and, wherever practicable, directly from the individual concerned.

Collection practices will be transparent and respectful, and individuals will be provided with sufficient information to understand:

1. why their information is being collected;
2. how the information will be used;
3. who it may be shared with;
4. whether providing the information is voluntary or mandatory;
5. the consequences of not providing requested information; and
6. how they may access or correct their information or make a privacy complaint.

The organisation will take reasonable steps to ensure that individuals understand these matters before or at the time information is collected, or as soon as reasonably practicable afterwards.

7.3 Collection Directly from Individuals

Wherever practicable, Reframe will collect personal information directly from the individual to whom the information relates.

Personal information may be collected through:

- a. conversations with employees or volunteers;
- b. telephone enquiries;
- c. email correspondence;
- d. online forms;
- e. service intake processes;
- f. referrals;
- g. fundraising activities;
- h. volunteer or employment applications;
- i. training registrations;
- j. events; and
- k. other interactions with Reframe.

Collecting information directly supports transparency, promotes information quality and enables individuals to make informed decisions regarding their privacy.

7.4 Anonymous and Pseudonymous Interactions

Reframe recognises that some individuals may wish to seek information or assistance without identifying themselves.

Where lawful and reasonably practicable, individuals may interact with Reframe anonymously or by using a pseudonym.

Examples may include:

- a. accessing publicly available information;
- b. attending community education sessions;
- c. making general enquiries; or
- d. seeking preliminary information regarding available services.

There will, however, be circumstances where identification is reasonably necessary, including where Reframe is providing ongoing support, responding to safeguarding concerns, administering donations, processing employment applications or complying with legal obligations.

Where anonymity cannot be maintained, Reframe will explain why identification is required and how personal information will be protected.

7.5 Collection from Third Parties

In limited circumstances, Reframe may collect personal information from a third party where doing so is lawful and reasonably necessary.

Examples include information received from:

- a. government agencies;
- b. police;
- c. healthcare providers;
- d. legal practitioners;
- e. specialist domestic and family violence services;
- f. child protection agencies;
- g. authorised representatives;
- h. family members acting with appropriate authority; or
- i. other organisations involved in supporting an individual.

Where information is collected from a third party, Reframe will, wherever practicable, notify the individual in accordance with the Australian Privacy Principles unless an exception under the *Privacy Act 1988 (Cth)* applies.

The organisation will also take reasonable steps to ensure that information obtained from third parties is accurate, relevant and appropriate before relying upon it.

7.6 Collection of Sensitive Information

Given the nature of Reframe's services, the organisation may collect sensitive information where it is reasonably necessary for the provision of support services, safeguarding, risk management or compliance with legal obligations.

Sensitive information may include:

- a. health information;
- b. disability information;
- c. information relating to domestic or family violence;
- d. counselling information;
- e. safety planning;
- f. cultural background where relevant;
- g. Aboriginal and Torres Strait Islander status where voluntarily provided;
- h. sexual orientation or gender identity where voluntarily disclosed;
- i. information relating to children; and
- j. other sensitive information as defined by the *Privacy Act 1988 (Cth)*.

Sensitive information will generally only be collected with the individual's consent unless another lawful basis for collection applies.

Because of the potential consequences of unauthorised disclosure, Reframe will apply enhanced privacy and security safeguards to all sensitive information.

7.7 Stories, Artwork and Lived Experience

Some individuals may choose to share personal stories, artwork, creative works or lived-experience accounts with Reframe. Providing this information is entirely voluntary, and individuals may choose to share as much or as little as they feel comfortable providing.

Reframe recognises that a personal story, artwork or lived-experience account may contain highly sensitive information, and may also include information about other people. Where practicable, Reframe will encourage contributors to consider the privacy of others when sharing such material.

Unless a contributor expressly agrees otherwise, providing a story, artwork or lived experience to Reframe does not automatically authorise Reframe to publish that material in an identifiable form.

7.8 Children and Young People

Reframe is mindful that its work brings it into contact with children and young people. Wherever practicable, Reframe will collect only the minimum information necessary where a child is involved, and will explain, in an age-appropriate way, why information is being collected.

Reframe does not knowingly collect personal information from a child through its website. Where a child's creative work, story or artwork is shared with Reframe, identifying information about the child will not be published without the consent of the child's parent, guardian or other authorised representative, except where the child is capable of providing informed consent and has done so.

7.9 Unsolicited Personal Information

From time to time, Reframe may receive personal information that it has not requested.

Where unsolicited personal information is received, Reframe will determine whether the information could have been lawfully collected had it been requested.

If the information is not reasonably necessary for Reframe's functions or activities and there is no lawful basis for retaining it, the organisation will securely destroy or permanently de-identify the information as soon as reasonably practicable, unless doing so would be unlawful or unreasonable.

7.10 Notification of Collection

At or before the time personal information is collected, or as soon as reasonably practicable afterwards, Reframe will take reasonable steps to notify individuals of the matters required by APP 5, including:

1. the identity and contact details of Reframe;
2. the purpose of collection;
3. the consequences of not providing information;
4. the usual disclosures of personal information;
5. any likely overseas disclosures;
6. the availability of this Privacy Policy; and
7. how to access or correct personal information or make a privacy complaint.

Collection notices will be written in clear and accessible language and, where appropriate, adapted to meet the communication needs of children, people with disability and individuals affected by trauma.

7.11 Data Minimisation

Reframe is committed to collecting only the minimum amount of personal information reasonably necessary to achieve a legitimate organisational purpose.

Personnel must not request or retain information simply because it may be useful in the future or because it has historically been collected. Before requesting personal information, consideration should be given to whether the relevant purpose can be achieved by collecting less information, using existing information already held by the organisation or relying on de-identified information.

This principle supports privacy by design, reduces organisational risk and strengthens compliance with the Australian Privacy Principles.

8. Use of Personal Information

8.1 Commitment to Appropriate Use

The Reframe Foundation Ltd recognises that individuals provide personal information with the expectation that it will be managed responsibly, respectfully and only for legitimate organisational purposes. The organisation is committed to ensuring that personal information is used in a manner that is consistent with the purpose for which it was collected, the reasonable expectations of the individual, and the requirements of the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles.

Reframe will not use personal information in a manner that is unfair, misleading or inconsistent with its charitable purpose. The organisation will ensure that all decisions relating to the use of personal information are guided by the principles of necessity, proportionality, transparency and respect for individual privacy.

8.2 Primary Purpose of Collection

Personal information will ordinarily be used only for the primary purpose for which it was collected. Depending on the nature of an individual's engagement with Reframe, this may include the delivery of support services, responding to enquiries, facilitating referrals, administering donations, recruiting employees or volunteers, managing governance obligations, complying with funding requirements or undertaking other activities directly connected with the organisation's charitable objectives.

The organisation will take reasonable steps to ensure that personal information remains accurate, relevant and up to date before it is used to make decisions affecting an individual or to deliver services on their behalf.

8.3 Secondary Use of Personal Information

Reframe may use personal information for a secondary purpose where that purpose is directly related to the primary purpose of collection and the individual would reasonably expect such use. Secondary use may also occur where the individual has provided informed consent or where the use is otherwise authorised or required by law.

In determining whether a proposed secondary use is appropriate, Reframe will consider the individual's reasonable expectations, the sensitivity of the information, the potential impact on the individual and whether the proposed use is consistent with the organisation's commitment to protecting privacy and promoting safety.

Where there is uncertainty regarding a proposed secondary use, advice should be sought from the Privacy Officer before the information is used.

8.4 Trauma-Informed Use of Information

Reframe acknowledges that the manner in which personal information is used can significantly affect the wellbeing and safety of victim-survivors of domestic and family violence. The organisation is committed to ensuring that personal information is used in a manner that supports recovery, empowerment and informed decision-making, while minimising the risk of re-traumatisation or unintended harm.

Before using sensitive information, personnel should consider whether the proposed use is necessary, whether less intrusive alternatives are available and whether the intended use could adversely affect the individual's safety or wellbeing. Where possible, individuals should be informed about significant uses of their information and involved in decisions regarding how that information is managed.

8.5 Use of Sensitive Information

Sensitive information will be used only where it is reasonably necessary for the purpose for which it was collected, where the individual has provided consent or where the use is otherwise authorised or required by law.

Given the nature of Reframe's services, sensitive information may be used to undertake risk assessments, develop safety plans, coordinate support services, respond to safeguarding concerns, comply with legal obligations or protect the health, safety or wellbeing of individuals. Access to

sensitive information will be restricted to authorised personnel who require the information to perform their duties.

Reframe will regularly review the categories of sensitive information it collects to ensure that only information that is reasonably necessary is retained.

8.6 De-identified Information

Wherever practicable, Reframe will use de-identified or aggregated information instead of identifiable personal information for purposes such as organisational planning, service evaluation, quality improvement, statistical reporting, research, advocacy and funding applications.

The organisation acknowledges that de-identification requires ongoing management and that information may become identifiable if combined with other data sources. Appropriate safeguards will therefore be maintained to minimise the risk of re-identification.

Where research activities involve identifiable personal information, Reframe will ensure that appropriate ethical, legal and privacy considerations are addressed before the research commences.

8.7 Stories, Artwork and Lived Experience

Where an individual has voluntarily shared a personal story, artwork, creative work or lived-experience account, Reframe will only use that material for the purpose for which it was provided, or a purpose the contributor has expressly agreed to.

Where Reframe wishes to publish identifiable material, it will seek the contributor's written permission before publication, unless publication is otherwise authorised or required by law. Contributors may request that their name not be published, that identifying information be removed, that a pseudonym be used, or that their contribution be published anonymously. Reframe will make reasonable efforts to honour these requests.

8.8 Fundraising and Direct Marketing

As a registered charity, Reframe may communicate with donors, supporters, volunteers and members of the community regarding fundraising campaigns, events, advocacy initiatives, publications and opportunities to support the organisation's work.

Direct marketing communications will only be undertaken in accordance with applicable legislation, including the *Privacy Act 1988 (Cth)* and, where relevant, the *Spam Act 2003 (Cth)*. Individuals will be provided with a simple and effective means of opting out of future marketing communications, and Reframe will promptly honour requests to unsubscribe or withdraw consent.

Reframe will not sell, rent or otherwise disclose personal information to third parties for commercial marketing purposes.

8.9 Research, Advocacy and Service Improvement

Reframe is committed to improving services for individuals affected by domestic and family violence and may use information to evaluate programs, identify emerging community needs, inform advocacy initiatives and demonstrate organisational impact.

Where information is used for these purposes, Reframe will use de-identified information wherever reasonably practicable. If identifiable personal information is required, the organisation will ensure that an appropriate legal basis exists for the proposed use and that the privacy, dignity and safety of affected individuals are protected.

Research, evaluation and advocacy activities should contribute to the organisation's charitable purpose and must not compromise the confidentiality or safety of individuals who have engaged with Reframe.

8.10 Artificial Intelligence and Emerging Technologies

Reframe recognises the increasing use of artificial intelligence and other emerging technologies in administrative and service delivery environments. The organisation is committed to ensuring that such technologies are implemented responsibly and do not compromise the privacy, safety or rights of individuals.

Identifiable personal information relating to victim-survivors, children or other vulnerable individuals must not be entered into publicly available artificial intelligence platforms unless the organisation has undertaken an appropriate privacy and security assessment and authorised the use of the technology. Any future use of artificial intelligence to support organisational activities will be subject to human oversight, appropriate governance and compliance with applicable privacy legislation.

9 Disclosure of Personal Information

9.1 Commitment to Responsible Disclosure

The Reframe Foundation Ltd recognises that the disclosure of personal information is one of the most significant privacy decisions the organisation may make. Individuals who engage with Reframe do so with the expectation that their personal information will remain confidential except where disclosure is necessary, lawful and consistent with this Policy.

Reframe is committed to ensuring that personal information is disclosed only where there is a legitimate organisational purpose, an appropriate legal basis for disclosure and adequate consideration has been given to the potential impacts on the individual concerned. Wherever practicable, only the minimum amount of personal information reasonably necessary to achieve the intended purpose will be disclosed.

The organisation acknowledges that inappropriate disclosure of information relating to domestic and family violence may expose victim-survivors, children and other individuals to significant risk of harm. Accordingly, decisions regarding disclosure must always be informed by a careful assessment of privacy, safety and legal obligations.

9.2 Disclosure with Consent

Reframe will ordinarily disclose personal information only with the informed consent of the individual concerned. Consent should be voluntary, current, specific and based on sufficient information to enable the individual to understand the nature and consequences of the proposed disclosure.

Where practicable, consent should identify the information to be disclosed, the person or organisation receiving the information, the purpose of the disclosure and any limitations or conditions that apply.

Reframe recognises that consent is an ongoing process rather than a single administrative event and that individuals may withdraw or vary their consent at any time, subject to any legal or practical limitations.

Before relying upon consent, personnel should consider whether the individual is able to provide informed consent freely and whether there are any factors, including trauma, coercion, language barriers or cognitive impairment, that may affect the individual's understanding or decision-making capacity.

9.3 Disclosure Required or Authorised by Law

There are circumstances in which Reframe may be required or authorised to disclose personal information without obtaining an individual's consent. Such disclosures may arise under Commonwealth, State or Territory legislation, through court orders or subpoenas, or in connection with lawful requests made by government agencies or regulatory authorities.

Reframe may also disclose personal information where disclosure is necessary to comply with mandatory reporting obligations, safeguarding responsibilities or other statutory duties.

Where disclosure is required or authorised by law, the organisation will ensure that only the information reasonably necessary to satisfy the legal requirement is disclosed. Wherever practicable and lawful, the Privacy Officer or another appropriately authorised officer should be consulted before information is released.

9.4 Serious Threats to Life, Health or Safety

Reframe acknowledges that circumstances may arise in which the disclosure of personal information is necessary to prevent or lessen a serious threat to the life, health or safety of an individual or the public. Decisions to disclose information under these circumstances must be based upon a reasonable belief that disclosure is necessary and proportionate to the identified risk.

In assessing whether disclosure is appropriate, Reframe will consider the immediacy and seriousness of the threat, the likelihood that disclosure will reduce the identified risk, the potential consequences of disclosure for the individual concerned and any alternative measures that may adequately address the situation.

Where disclosure occurs to protect life, health or safety, the organisation will maintain appropriate records of the decision-making process and the information disclosed.

9.5 Information Sharing with Service Providers and Partners

The effective delivery of services may require Reframe to share personal information with external organisations involved in supporting an individual. This may include government agencies, specialist domestic and family violence services, healthcare providers, legal practitioners, counsellors, emergency accommodation providers or other organisations providing integrated support.

Information sharing will occur only where there is an appropriate legal basis and where the disclosure is reasonably necessary to support the individual's care, safety or wellbeing, facilitate a referral, coordinate services or otherwise fulfil Reframe's functions.

Before sharing information, Reframe will consider whether the receiving organisation has appropriate privacy and information security practices and whether the proposed disclosure is proportionate to the purpose for which the information is being shared.

9.6 Protection of Victim-Survivor Information

Information concerning victim-survivors of domestic and family violence requires the highest standard of confidentiality. Before disclosing such information, Reframe will carefully assess whether disclosure could reveal an individual's location, compromise a safety plan, expose confidential accommodation, facilitate coercive control or otherwise increase the risk of harm.

Where there is uncertainty regarding the potential consequences of disclosure, Reframe will adopt a precautionary approach that prioritises safety while remaining consistent with legal obligations. Personnel should seek advice from the Privacy Officer or an appropriately authorised manager before proceeding with any disclosure that may present heightened risks.

The organisation recognises that disclosures involving children require particular care and will ensure that decisions involving children are informed by the child's best interests, applicable child protection legislation and relevant safeguarding policies.

9.7 Related Entities

Reframe may share personal information with related entities where reasonably necessary for operational purposes. Any related entity receiving personal information will be expected to maintain privacy protections that are at least equivalent to those set out in this Policy.

9.8 Stories, Artwork and Creative Works

Where an individual has voluntarily submitted artwork, a creative work, a lived-experience account or a personal story, Reframe will not disclose or publish that material in an identifiable form without the contributor's permission, unless disclosure is otherwise authorised or required by law.

Reframe recognises that a contributor's consent to publication may change over time. Where reasonably practicable, contributors may contact Reframe to request that identifying information be removed from previously published material, recognising that complete removal may not always be possible where material has already been lawfully published or distributed.

9.9 Overseas Disclosure

Reframe primarily stores personal information within Australia; however, some information may be processed or stored by reputable cloud service providers whose infrastructure operates internationally.

Before engaging service providers that may transfer or store personal information outside Australia, Reframe will undertake appropriate due diligence to ensure that the provider maintains privacy and security standards substantially equivalent to those required under Australian privacy law. Contractual arrangements should require service providers to implement appropriate safeguards, maintain confidentiality and notify Reframe of any actual or suspected security incidents affecting personal information.

Where overseas disclosure is likely to occur, Reframe will take reasonable steps to inform individuals through this Policy and associated collection notices in accordance with the Australian Privacy Principles.

9.10 Accountability and Record Keeping

Significant disclosures of personal information should be appropriately documented to support accountability, transparency and organisational learning. Records should identify the legal basis for the disclosure, the information disclosed, the recipient of the information, the purpose of the disclosure and any relevant risk considerations.

Reframe recognises that effective record keeping supports sound governance and enables the organisation to demonstrate compliance with its privacy obligations. Information relating to disclosures will be retained in accordance with the organisation's records management framework and any applicable legislative requirements.

10. Information Sharing in the Domestic and Family Violence Context

10.1 Purpose

The Reframe Foundation Ltd recognises that the lawful and appropriate sharing of information may be necessary to promote the safety, wellbeing and recovery of individuals affected by domestic and family violence. At the same time, the organisation acknowledges that inappropriate or unnecessary disclosure of personal information may expose victim-survivors, children and other individuals to significant physical, psychological or emotional harm.

This section establishes the governance principles that apply to decisions regarding information sharing in the context of domestic and family violence.

10.2 Guiding Principles

Reframe will ensure that decisions to share personal information are guided by the following principles:

- a. the safety and wellbeing of victim-survivors, children and other affected persons is the primary consideration;
- b. information will only be shared where there is a lawful basis for doing so;
- c. only the minimum amount of personal information reasonably necessary to achieve the intended purpose will be disclosed;
- d. information sharing decisions will be proportionate to the identified risks;
- e. information will be shared only with organisations or individuals who have a legitimate need to receive the information; and
- f. all significant information sharing decisions will be appropriately documented.

10.3 Lawful Information Sharing

Reframe may share personal information where:

- a. the individual has provided informed consent;
- b. the disclosure is reasonably necessary for the primary purpose for which the information was collected or a directly related secondary purpose reasonably expected by the individual;

- c. disclosure is authorised or required by Commonwealth, State or Territory legislation;
- d. disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of an individual or the public; or
- e. another exception under the *Privacy Act 1988 (Cth)* applies.

Before sharing information, Reframe will consider whether the intended purpose can be achieved using de-identified information or by disclosing less information.

10.4 Safety-Focused Decision Making

Before disclosing information relating to a victim-survivor or child, personnel must consider whether disclosure could:

1. reveal a confidential address or refuge location;
2. compromise an existing safety plan;
3. expose an individual to further violence;
4. facilitate coercive control or stalking;
5. reveal information to a perpetrator;
6. prejudice ongoing investigations or legal proceedings; or
7. otherwise increase the risk of harm.

Where uncertainty exists, advice should be obtained from the Privacy Officer or an appropriately authorised senior officer before disclosure occurs.

10.5 Information Sharing with Partner Organisations

Reframe works collaboratively with government agencies, specialist domestic and family violence services, health practitioners, legal services and other community organisations.

Information sharing arrangements should be supported by appropriate governance mechanisms, including confidentiality obligations, information sharing agreements where appropriate, and reasonable assurance that recipient organisations maintain suitable privacy and information security practices.

10.6 Documentation

Significant information sharing decisions should be documented to demonstrate:

- a. the legal authority relied upon;
- b. the purpose of the disclosure;
- c. the information disclosed;
- d. the recipient;
- e. the safety considerations assessed;
- f. any conditions placed upon the disclosure; and
- g. the decision-maker.

Maintaining accurate records promotes accountability, transparency and organisational learning.

11. Information Security and Records Management

11.1 Commitment to Information Security

The Reframe Foundation Ltd recognises that effective information security is fundamental to protecting the privacy, dignity and safety of the individuals who engage with the organisation. As a provider of services to victim-survivors of domestic and family violence, Reframe acknowledges that unauthorised access to personal information may expose individuals to significant physical, psychological, financial or reputational harm.

Reframe is committed to implementing and maintaining an information security framework that is proportionate to the nature, volume and sensitivity of the personal information it holds. Information security measures will be regularly reviewed to ensure they remain appropriate, effective and responsive to evolving cyber security threats, technological developments and changes to the organisation's operations.

The organisation recognises that information security is a shared responsibility and that every person handling personal information contributes to protecting the confidentiality, integrity and availability of that information.

11.2 Protection of Personal Information

Reframe will take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure throughout the information lifecycle.

Protective measures adopted by the organisation may include administrative, physical and technical safeguards appropriate to the sensitivity of the information concerned. Such safeguards will be designed to ensure that personal information remains available to authorised personnel when required while protecting individuals from unnecessary privacy risks.

Security controls will be regularly evaluated having regard to the volume of information held, emerging cyber security risks, legislative developments and recognised industry practice.

11.3 Access Management

Access to personal information will be restricted to individuals who require access to perform their authorised duties. Access permissions will be granted on the basis of business need and the principle of least privilege, ensuring that personnel have access only to the information necessary to fulfil their responsibilities.

Reframe will implement appropriate processes to authorise, review and revoke access to information systems. Access privileges will be reviewed periodically and adjusted where an individual's role changes or where access is no longer required.

Individuals authorised to access personal information are expected to maintain strict confidentiality and must not access information for personal interest, curiosity or any purpose unrelated to their responsibilities.

11.4 Physical and Electronic Security

Reframe will implement appropriate physical and electronic safeguards to protect personal information against unauthorised access and accidental loss.

Physical records containing personal information will be stored in secure locations with access restricted to authorised personnel. Electronic information will be managed using secure information systems that incorporate appropriate authentication, monitoring and backup arrangements.

Where reasonably practicable, the organisation will implement measures such as multi-factor authentication, encryption, secure password management, system monitoring and regular software updates to reduce the likelihood of unauthorised access or cyber security incidents.

The organisation acknowledges that information security is an evolving discipline and will continue to assess emerging technologies and security practices that may strengthen the protection of personal information.

11.5 Remote Working and Digital Environments

Reframe recognises that employees and volunteers may undertake authorised work from locations outside the organisation's premises. Personal information accessed or managed in remote working environments must receive the same level of protection as information handled within organisational facilities.

Appropriate governance arrangements will be implemented to support the secure use of organisational devices, remote access technologies and cloud-based systems. Personnel are expected to exercise appropriate care when accessing personal information outside the workplace and to ensure that confidential information cannot be viewed or accessed by unauthorised persons.

The organisation will periodically review remote working arrangements to ensure that they continue to support privacy, cyber security and information governance requirements.

11.6 Records Management

Reframe is committed to maintaining records that are accurate, reliable, complete and capable of supporting informed decision-making, organisational accountability and legislative compliance.

Records will be created and maintained in accordance with recognised records management principles and any applicable legislative requirements. Personal information should be recorded objectively, accurately and respectfully, avoiding unnecessary or speculative commentary. Records should contain sufficient information to support the organisation's activities while avoiding the collection or retention of information that is not reasonably necessary.

The organisation will maintain governance arrangements to ensure that records remain authentic, accessible and appropriately protected throughout their lifecycle.

11.7 Information Quality

Reframe acknowledges that decisions affecting individuals should be based upon information that is accurate, complete, relevant and current.

Reasonable steps will be taken to ensure that personal information is reviewed and updated where necessary, particularly where the information is relied upon to deliver services, assess risk, make organisational decisions or comply with legal obligations.

Individuals are encouraged to advise Reframe if their personal information changes or if they believe information held by the organisation is inaccurate or incomplete. Requests to correct personal information will be managed in accordance with Section 12 of this Policy.

11.8 Retention of Personal Information

Reframe will retain personal information only for as long as it is reasonably required to fulfil the purpose for which it was collected or to satisfy applicable legislative, contractual, financial or operational requirements.

Retention periods will be determined having regard to the nature of the information, applicable legislation, funding requirements, potential legal proceedings, child safeguarding considerations and recognised records management principles.

The organisation recognises that retaining personal information longer than necessary may increase privacy risks and will periodically review the information it holds to determine whether continued retention remains justified.

11.9 Secure Destruction and De-identification

Where personal information is no longer required and there is no legal or operational basis for its continued retention, Reframe will take reasonable steps to securely destroy or permanently de-identify the information.

Secure destruction methods will be appropriate to the format and sensitivity of the information and may include confidential destruction of paper records, secure deletion of electronic information, cryptographic erasure of digital storage media or permanent de-identification of information used for research, evaluation or statistical purposes.

The organisation will ensure that disposal processes minimise the risk of unauthorised access, disclosure or reconstruction of personal information.

11.10 Privacy by Design

Reframe is committed to embedding privacy considerations into organisational governance, strategic planning and operational decision-making.

Privacy should be considered whenever the organisation introduces new programs, technologies, partnerships, digital platforms, fundraising initiatives, databases or administrative processes that involve the handling of personal information.

Where a proposed initiative is likely to create a significant privacy risk, Reframe will undertake an appropriate privacy impact assessment before implementation. The assessment should consider the necessity of collecting personal information, potential privacy impacts, opportunities to minimise information collection and appropriate security measures.

Embedding privacy into organisational design supports legislative compliance, strengthens public confidence and reduces the likelihood of future privacy incidents.

11.11 Information Governance

Reframe recognises that effective privacy protection forms part of broader information governance.

The organisation will maintain governance arrangements that promote responsible information management, accountability, transparency and continuous improvement. Information governance includes oversight of privacy, cyber security, records management, information quality, retention, disposal and compliance with legislative obligations.

The Board of Directors will receive periodic reporting regarding significant privacy risks, information governance matters and privacy incidents to support informed oversight of the organisation's governance responsibilities.

12. Privacy Rights, Governance and Continuous Improvement

12.1 Commitment to Individual Privacy Rights

The Reframe Foundation Ltd recognises that individuals have the right to understand how their personal information is managed and to exercise appropriate control over that information. Reframe is committed to respecting these rights and ensuring that individuals are provided with reasonable opportunities to access, correct and, where appropriate, challenge the way their personal information is handled.

The organisation acknowledges that respecting individual privacy rights contributes to transparency, accountability and public confidence in its services. Requests concerning personal information will be managed fairly, consistently and in accordance with the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles.

12.2 Access to Personal Information

Subject to applicable legislation, individuals may request access to the personal information held about them by Reframe.

Requests for access should be made to the Privacy Officer using the contact details published by the organisation. Reframe may require reasonable proof of identity before granting access to ensure that personal information is released only to the individual concerned or to a person lawfully authorised to act on their behalf.

The organisation will respond to requests within a reasonable period and, where practicable, within thirty (30) calendar days. Access will generally be provided in the form requested by the individual unless doing so is impracticable or another lawful means of providing access is more appropriate.

Reframe recognises that access to personal information promotes transparency and supports individuals in understanding how their information is managed.

12.3 Circumstances Where Access May Be Refused

While Reframe supports openness wherever possible, there are limited circumstances in which access to personal information may be refused in accordance with the *Privacy Act 1988 (Cth)*.

Access may be refused where providing access would unreasonably affect the privacy of another person, prejudice legal proceedings, reveal information protected by legal professional privilege, create a serious threat to the life, health or safety of an individual, prejudice law enforcement activities or where another exception recognised by law applies.

Where access is refused, Reframe will provide written reasons for the decision and information regarding any available complaint or review mechanisms, unless doing so would itself be unlawful.

12.4 Correction of Personal Information

Reframe is committed to ensuring that the personal information it holds is accurate, complete, relevant and up to date.

Individuals may request correction of information that they believe is inaccurate, incomplete, misleading or no longer current. Upon receiving such a request, Reframe will assess the available information and, where appropriate, amend its records as soon as reasonably practicable.

Where Reframe determines that a requested correction should not be made, the organisation will provide the individual with written reasons for the decision and information about available review or complaint mechanisms. Where appropriate, Reframe will also take reasonable steps to associate a statement with the information indicating that the individual disputes its accuracy.

12.5 No Fee for Privacy Requests

Reframe does not ordinarily charge a fee for requests to access or correct personal information. However, where permitted by law, Reframe may charge a reasonable fee to cover the administrative cost of responding to a request that is extensive, complex or requires a substantial amount of staff time.

12.6 Withdrawal of Consent

Where Reframe relies on an individual's consent to collect, use or disclose personal information, that consent may generally be withdrawn at any time by contacting the organisation.

Withdrawal of consent will not affect actions lawfully undertaken before consent was withdrawn. However, individuals should be advised that withdrawing consent may affect Reframe's ability to continue providing certain services or to fulfil obligations arising from the individual's request.

Where consent relates to the publication of lived experience stories, photographs or creative works, Reframe will work collaboratively with the individual to determine the most appropriate response. While the organisation will take reasonable steps to honour requests wherever practicable, complete removal may not always be possible where material has already been lawfully published, distributed or incorporated into educational resources.

12.7 Privacy Incidents and Eligible Data Breaches

Reframe acknowledges that, despite appropriate governance arrangements, privacy incidents may occur. The organisation is committed to responding promptly to any actual or suspected privacy incident in order to minimise harm, restore security and strengthen organisational practices.

All personnel must report suspected privacy incidents immediately upon becoming aware of them. Privacy incidents will be assessed to determine their nature, scope and potential impact on affected individuals. Where an incident is likely to constitute an Eligible Data Breach under the *Privacy Act 1988 (Cth)*, Reframe will comply with the requirements of the Notifiable Data Breaches Scheme, including assessment, notification of affected individuals and notification to the Office of the Australian Information Commissioner where required.

Following any significant privacy incident, the organisation will review the circumstances giving rise to the incident and implement appropriate corrective actions to reduce the likelihood of recurrence.

12.8 Privacy Complaints

Reframe encourages individuals to raise concerns regarding the management of their personal information at the earliest opportunity. Privacy complaints provide valuable opportunities to improve organisational practices and strengthen public confidence in the organisation's privacy management framework.

Complaints should be directed to the Privacy Officer and will be managed in a fair, impartial and timely manner. Upon receipt of a complaint, Reframe will acknowledge the complaint, undertake an appropriate investigation, consider all relevant information and provide the complainant with a written response outlining the outcome of the investigation and any actions taken.

Where a complainant remains dissatisfied with Reframe's response, they may refer the matter to the Office of the Australian Information Commissioner or another authority with jurisdiction to consider the complaint.

12.9 Privacy Officer

The Board will appoint a Privacy Officer to oversee the implementation of this Policy and the organisation's broader privacy management framework.

The Privacy Officer is responsible for promoting compliance with privacy legislation, providing advice to personnel, coordinating responses to privacy incidents and complaints, monitoring legislative developments, supporting Privacy Impact Assessments, overseeing privacy training and reporting significant privacy matters to senior management and the Board.

The appointment of a Privacy Officer does not diminish the responsibility of all personnel to comply with this Policy and applicable privacy legislation.

12.10 Roles and Responsibilities

Privacy governance is a shared responsibility across the organisation.

The **Board of Directors** is responsible for establishing the organisation's privacy governance framework, approving this Policy, overseeing strategic privacy risks and ensuring that appropriate resources are available to support compliance.

The **Chief Executive Officer** is responsible for implementing this Policy, promoting a culture of privacy and ensuring that privacy risks are effectively managed across the organisation.

The **Privacy Officer** is responsible for monitoring compliance, coordinating privacy incident responses, managing complaints, providing advice and supporting continuous improvement.

Managers are responsible for ensuring that privacy obligations are understood within their areas of responsibility, that personnel receive appropriate training and that privacy risks are identified and managed effectively.

Employees, volunteers, contractors and consultants are responsible for complying with this Policy, maintaining confidentiality, participating in required training, reporting privacy incidents and handling personal information respectfully and lawfully.

12.11 Monitoring, Assurance and Continuous Improvement

Reframe is committed to maintaining an effective and contemporary privacy management framework.

The organisation will monitor compliance with this Policy through internal reporting, management review, privacy incident reporting, periodic audits, risk assessments, staff training and ongoing evaluation of organisational practices. Lessons learned from complaints, data breaches, legislative developments and stakeholder feedback will be incorporated into future improvements to privacy governance.

Privacy should be considered an integral component of organisational governance, strategic planning and risk management. The Board will receive periodic reports regarding significant privacy risks, privacy incidents and emerging legislative developments to support informed oversight and continuous improvement.

12.12 Policy Review

This Policy will be reviewed at least every two years, or earlier where there are significant changes to legislation, organisational operations, technology, funding arrangements or identified privacy risks.

Any amendments to this Policy must be approved by the Board of Directors.

The most current version of the Policy will be published on Reframe's website and made available to any person upon request.

13. Document Control

Document	Privacy Policy	Version	Date	Summary
Organisation	The Reframe Foundation Ltd	1.0	July 2025	Initial Privacy Policy
Policy Owner	Privacy Officer	2.0	July 2026	Revised Privacy Policy

Document Privacy Policy

Approved By Board of Directors

Version 2.0

Classification Public

Effective Date 30 July, 2026

Review Date Every two years

Version History

Appendix A – Mapping to the Australian Privacy Principles

The following table demonstrates how The Reframe Foundation Ltd has incorporated the Australian Privacy Principles (APPs) into its privacy governance framework.

Australian Privacy Principle	Privacy Policy Reference	Summary of Compliance
APP 1 – Open and Transparent Management of Personal Information	Sections 1, 2, 4, 11	Establishes governance framework, commitment to privacy, responsibilities and public availability of the Privacy Policy.
APP 2 – Anonymity and Pseudonymity	Section 7.4	Individuals may interact anonymously or using a pseudonym where lawful and practicable.
APP 3 – Collection of Solicited Personal Information	Section 7	Limits collection to information reasonably necessary for Reframe's functions and activities.
APP 4 – Dealing with Unsolicited Personal Information	Section 7.9	Requires assessment and secure destruction or de-identification where unsolicited information is not required.
APP 5 – Notification of the Collection of Personal Information	Section 7.10	Individuals are informed of the purpose of collection, use, disclosures, rights and this Privacy Policy.
APP 6 – Use or Disclosure of Personal Information	Sections 8 and 9	Personal information is used and disclosed only for lawful purposes, with consent or where authorised or required by law.
APP 7 – Direct Marketing	Section 8.8	Marketing communications comply with applicable legislation and include opt-out mechanisms. Personal

Australian Privacy Principle	Privacy Policy Reference	Summary of Compliance
		information is not sold or disclosed for commercial marketing.
APP 8 – Cross-border Disclosure of Personal Information	Section 9.9	Overseas disclosures are subject to due diligence and appropriate contractual safeguards.
APP 9 – Adoption, Use or Disclosure of Government Related Identifiers	Privacy Procedure	Government-related identifiers will only be collected, used or disclosed where authorised or required by law. Operational requirements are contained within the Privacy Procedure.
APP 10 – Quality of Personal Information	Section 11.7	Reframe takes reasonable steps to ensure personal information is accurate, complete, relevant and current.
APP 11 – Security of Personal Information	Section 11	Establishes governance requirements for information security, access controls, records management, retention and secure destruction.
APP 12 – Access to Personal Information	Section 12.2	Individuals may request access to their personal information in accordance with the Privacy Act 1988 (Cth).
APP 13 – Correction of Personal Information	Section 12.4	Individuals may request correction of inaccurate, incomplete or out-of-date information.