Lifeline South Coast
Privacy Policy

Version 8.0
Release Date: DECEMBER 2025
Review Date: AUGUST 2026

Table of contents

1 Document History

Version	Document Owner	Approved By	Date Approved	Review Date	Comments
3.0	Irene Wilkins		October 2008		
3.1	Clare Leslie		July 2012		No doc changes – formatted in line with new LLSC Policy Template
3.2	Renee Green		May 2013		Updated Privacy Officer only
4.0	Renee Green Governance, Risk & Admin Mgr	Board	12/09/2016	30/09/2017	Adoption of LLA policy
4.1	Renee Green Governance, Risk & Admin Mgr	Board	25/09/2017	30/09/2018	No changes
5.0	Renee Green Finance & Governance Mgr	Board	26/11/2018	30/11/2020	Significant re-write giving consideration to legislative changes and community expectations
6.0	Finance & Governance Mgr	Board			Additional information added to include Financial Counselling Service
7.0	Denae Holland Finance & Governance Mgr	Board	22/11/2021	30/11/2023	Review of Policy by Management Team
7.1	Denae Holland Finance & Governance Mgr	Board	22/01/2024	30/11/2025	Application of compliance with APP's Update of LLA Privacy Policy
8.0	Denae Holland Finance & Governance Mgr	Board	19/03/2026	30/08/2028	Addition of section 4.12 Notifiable Data Breach

2 Introduction

Lifeline South Coast is committed to protecting the privacy of personal information which it collects, holds, and administers in accordance with the Privacy Act 1988 and the Australian Privacy Principles (APPs) contained within.

3 Definitions

Personal Information	Personal information includes a broad range of information, or an opinion, that could identify an individual:

	• an individual's name, signature, address, phone number or date of birth • sensitive information • credit information • employee record information • photographs • internet protocol (IP) addresses • voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique) location information from a mobile device (because it can reveal user activity patterns and habits)
Sensitive Information	Sensitive information is personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • some aspects of biometric information
Health Information	Health information' includes information or opinions about a person's: • physical and mental health • disability (at any time) • health preferences (including future provision of health services) • use of health services • bodily donations (for example, blood, organs), and • genetics
Crisis Supporter	A crisis supporter is a person who interacts directly with the help seeker when providing Lifeline Crisis Support services.
Australian Privacy Principles	There are 13 Australian Privacy Principles (APPs) and they govern standards, rights and obligations around: • the collection, use and disclosure of personal information • an organisation or agency's governance and accountability • integrity and correction of personal information • the rights of individuals to access their personal information.

4 Purpose

The purpose of this policy is to provide a framework for Lifeline South Coast in dealing with privacy considerations.

This Privacy Policy provides information and aims to be transparent around how Lifeline South Coast collects, handles and safeguards personal information. It also outlines how you can seek to access and correct your personal information and make a privacy complaint.

Appendix A to this Privacy Policy demonstrates Lifeline South Coast's compliance with the Australian Privacy Principles (APPs).

5 Policy

The primary way Lifeline South Coast collects personal information is when it is provided directly by individuals who interact with the organisation in any capacity. This includes, but is not limited to, people accessing our services, one-off or returning volunteers, contractors, paid staff members, donors, supporters, partners, and other individuals or representatives of organisations engaging with Lifeline South Coast.

The type of personal information collected will depend on the nature, purpose, and frequency of the interaction. Lifeline South Coast may also identify and engage with individuals and organisations whose values align with our mission, including through targeted and scalable marketing and engagement activities, training, and development purposes.

Where information is not provided directly, we may also use additional search methods, including external contacts and search engines such as social media and subscription based third party providers, to obtain supplementary information. Any information collected this way will be relevant to our purpose and obtained in accordance with the providers outlined policies.

<u>Activities where we collect personal information include:</u>

- providing crisis support and suicide prevention services;
- conducting education and training in suicide prevention, crisis support and mental health and wellbeing to Lifeline Crisis Supporters and external individuals and organisations;
- conducting research and evaluation and assurance activities to ensure the delivery of quality services and achieve continuous improvement in service delivery;
- training of Crisis Supporters and front-line workers to support individuals impacted by domestic violence, and Lifeline employees and contractors in other supporting programs. This includes trainers and students;
- conducting fundraising activities to raise funds to support the services of the Lifeline South Coast;
- receiving a donation from you;
- assessing suitable candidates for career opportunities within Lifeline South Coast and managing your employment with us if you are an employee;

- assessing suitable candidates for volunteering opportunities within Lifeline South Coast;
- communicating with the public and the media, including through websites and social media, to raise public awareness of Lifeline services; and
- conducting investigations, and managing responses, in relation to complaints concerning Lifeline services and the operations of Lifeline South Coast.
- Complying with our legal obligations; and
- Assisting investigations and information requests from third parties, such as the police or the coroner, in accordance with the law.

5.1 ANONYMOUS INTERACTIONS

Where possible, Lifeline South Coast will allow you to interact anonymously unless it is impractical, or an applicable Australian law requires us to only deal with an identified individual.

You can choose the information you provide, however some information that makes you reasonably identifiable may be collected.

If you choose not to share the information we request or to identify yourself, we may not be able to provide you with some or all our services.

5.2 USE FOR PRIMARY PURPOSE AND CERTAIN SECONDARY PURPOSES

Lifeline South Coast must only use individuals' personal information for the primary purpose for which it was collected, a secondary purpose to which the individual has consented, or for a purpose related to the primary purpose of collection and the individual would reasonably expect the personal information to be used for such purpose.

Primary purposes (and secondary purposes for which consent is required) should be set out in collection notices, and may include:

Crisis Support Services	Providing crisis support and suicide prevention services to all Australians suffering emotional distress.
Service Quality	Recording interactions between Crisis Supporters or other Lifeline staff and the individual for the purpose of service quality, training, and improvement purposes in relation to Lifeline Australia's services.
Training	Delivering accredited training programs to students under the Lifeline Australia RTO and delivering non-accredited training programs to our community and other organisations, and for related program quality and continuous improvement purposes. This includes trainers and students.
Information Requests	Supporting Lifeline Australia and Lifeline South Coast's requirements in relation to investigating and facilitating the complaints process, in addition to assisting information requests from third parties, such as the police or the coroner, to undertake investigations.

Marketing & Fundraising	Communicating with individuals about donations, products, services, campaigns, causes, and events.
Research	Conducting and/or fund research into Lifeline Australia and Lifeline South Coast's programs and services or research into supporter attitudes and understanding how to improve crisis support services.
Volunteering & Other Support	Enabling individuals to assist with volunteering, community fundraising, advocacy, or other activities where community's assistance is sought.
Other Issues	Communicating with individuals in relation to Lifeline South Coast operations, activities, and objectives, to verify their identity, to improve and evaluate programs and services and comply with relevant laws.

Table information extract from Lifeline Australia Privacy Policy v3.4

5.3 DISCLOSURE OF PERSONAL INFORMATION

In addition to section 4.2, APP section 6.2 applies in relation to the use of personal information about an individual if:

- Disclosure of the information is required or authorised under an Australian law,
- A permitted general situation exists in relation to the use or disclosure of the information by us,
- If a permitted health situation exists in relation to use or disclosure of the information,
- We reasonably believe that the disclosure of the information is reasonably necessary for one or more enforcement body related activities.

In accordance with the *Privacy Act 1988, subsection 16B(2)*, where personal information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, we must take reasonable steps to ensure that the information is de-identified prior to disclosing that information in accordance with APP 6.1 or 6.2.

5.4 CONSENT TO COLLECT AND USE PERSONAL INFORMATION

Consent for recording of interactions

Lifeline Australia may record calls received on its crisis support telephone lines for the primary purposes described above. Lifeline Australia does record calls received through 13 11 14, 13 YARN, CAREinMIND, MensLine Australia, MindHealth Regional Access, the Suicide Call Back Service, and SuicideLine Victoria.

Lifeline may use the call recording for the primary purposes, but only where the individual has been clearly informed that the call will be recorded, and the relevant individual has consented to the call recording.

How consent will be obtained

At the beginning of the call	Individuals whose personal information is collected will be notified using an Interactive Voice Response (IVR) which references this Privacy Policy prior to being connected to a Crisis Supporter. Individuals are taken to consent to the call recording for Lifeline's primary purpose unless once connected, they ask the Crisis Supporter to stop recording at the beginning of the call.
During the call	If individuals wish to terminate the call recording during their call with the Crisis Supporter or counsellor, they may request the Crisis Supporter or counsellor to terminate the recording. Any portion of the call recorded until the point of termination will be maintained by Lifeline Australia in accordance with this Privacy Policy.

Table: Lifeline Australia Privacy Policy v3.4

In relation to employees and volunteers of Lifeline using a Lifeline Australia service:

- Employees and volunteers conducting a call that is recorded must be provided with a written notice that the calls they answer on the service line will be recorded and of the primary purposes of the call recording.
- Employees and volunteers will be given reasonable opportunity to give their consent to the call recording.

Consent for direct marketing

Lifeline South Coast may use individuals' personal information for direct marketing purposes, but only where:

- The direct marketing communication contains a prominent statement that the individual may opt out of receiving that type of communication, and
- The relevant individual has not made such a request.

Individuals whose personal information is collected using a collection notice that references this Privacy Policy are taken to consent to the use of their personal information for direct marketing purposes unless they have specifically opted out.

Opting out of direct marketing

Email direct marketing communications should contain an 'unsubscribe' link that provides individuals with the opportunity to opt out of direct marketing communications. In other circumstances, individuals who do not wish to receive direct marketing communications from Lifeline South Coast may contact us at (02) 4228 1311 or admin@llsc.org.au to opt out or use the opt out provided on the direct marketing material.

Lifeline South Coast must take all necessary steps to opt such individuals out of direct marketing communications. Requests to opt out of direct marketing communications should be treated in the first instance as a request to opt out of the campaign or event to which the communication relates. However, individuals must be given the opportunity to contact Lifeline South Coast (for example, by phone) to opt out of all direct marketing communications, across all programs, events, and channels.

Individuals have the right to request that Lifeline South Coast do not use or disclose personal information that may have been collected for the purpose of direct marketing, as well as request Lifeline South Coast to provide how the personal information was obtained. Lifeline South Coast will endeavour to respond to requests of this kind within a reasonable timeframe unless it is impractical to do so.

Removal of opt-outs
Individuals who register for events, make a donation or otherwise provide their personal information for marketing-related purposes after they have previously opted out of direct marketing communications should be taken to have 'opted in' once again and may receive direct marketing communications. However, all such direct marketing communications must give the individual the opportunity to opt out as described above.

5.5 COLLECTION AND USE OF PERSONAL INFORMATION

5.5.1 Information Collected

Lifeline South Coast tries to only collect personal information that is reasonable and necessary for, or directly related to, an activity we are undertaking to carry out our objectives. This may include, but not limited to, when you contact us:

- via telephone, in person, email, social media or website;
- when you join our customer loyalty program;
- when you register for training.

The kind of personal information we may collect, and its uses are described below.

Information collected in provision of a Lifeline crisis support telephone service
Lifeline collects information you provide to the voice support service through providing services to you.

Personal information, such as your name and contact details, will not be recorded unless you provide this information to Lifeline, or if this information is otherwise captured by its systems or call recordings. The following personal information which may include your sensitive such as health information, may be collected depending on your interaction with Lifeline:

Your name or the names of people you tell Lifeline about	Such as friends or family you are concerned about.
Your telephone number	If you use Lifeline's text-based service, then this will be used to communicate with you. Lifeline's telephone system might also display the number you call us from, or you might give your number to Lifeline for Lifeline Australia to contact you again.

Your address or location	If Lifeline need to make sure you are in a safe space, or if Lifeline need to support you by asking authorities to visit your location.
Details about you and others which are relevant to the call	For example, if you tell Lifeline about your health, about the loss of a loved one, about a drug or alcohol problem affecting you or someone you know, or if you are thinking about suicide or are worried that someone you know might attempt suicide. Lifeline take notes about the things you say to us so that we can figure out the best way to help you.
If Lifeline make a care plan for you	Then Lifeline might make notes about the actions recommended for you to take or the information given to you.
If you use Lifeline's telephone service, then the system will record and store any information	Noises or other sounds captured by the call recording, in addition to call time and duration, originating area of the call, and telephone number (if unblocked). This information is stored separately to other information Lifeline collect when individuals access its services.

Table: Lifeline Australia Privacy Policy v3.2

These records are stored in a system managed and maintained by Lifeline Australia.

Information collected when you volunteer

Personal or sensitive information necessary to enable us to assess your application is collected. Depending on the role, this may include:

- Your resume, statement addressing the criteria and referee reports
- Proof of Australian citizenship or residency
- Employment and volunteer history
- Copies of academic qualifications
- Criminal history and/or a working with children background check
- Health related information supplied by an employee or their medical practitioner
- Information relating to training and development

Volunteers for Board member positions may also have to provide information relevant to assessing conflict of interests and ACNC disclosure.

Information collected when you seek employment

We collect personal or sensitive information necessary to enable us to assess your application for employment, such as

- Resume, statement addressing the criteria and referee reports
- Written tasks undertaken by you during the selection process
- Copies of academic qualifications
- Criminal history and/or a working with children background check

Information collected in relation to employment

- Employment contract
- Information collected in relation to employment

- Proof of Australian citizenship or residency
- Copies of academic qualifications
- Health related information supplied by an employee or their medical practitioner
- Taxation details
- Banking details
- Superannuation details
- Information relating to training and development

As an employer Lifeline South Coast is a TFN recipient in accordance with s17 of the Privacy Act 1988, Privacy (Tax File Number) Rule 2015. Under the TFN Rule, a TFN recipient must not record, collect, use, or disclose TFN information unless this is permitted under taxation, personal assistance or superannuation law.

Lifeline Australia facilitates the use of a Workforce Management System (WFMS) by the Lifeline Members for the purpose of forecasting call demand and the allocation of resources across the Lifeline Member network (to support voice and digital (text and chat) services).

The WFMS holds details of each Crisis Supporter's name and contact details; skills and training, rostered shifts, and employment status (employee or volunteer).

Information collected in relation to CSWT, DV and Other Training

We collect personal information such as student contact details, Unique Student Identifier (USI), enrolment forms and academic records which are required by law to be collected on behalf of Lifeline Australia as a Registered Training Organisation (RTO).

This is following the Lifeline Australia RTO Compliance Manual. RTO number is 88036.

We collect information from trainers and assessors to verify they possess the requisite qualifications to deliver training and education.

Information collected when you seek Financial Counselling Services

The Financial Counselling service closed on 30th June 2023. Personal information was collected during the operation of the service, records are archived for seven years.

Personal information collected included address, date of birth, living arrangements, income, employment, cultural background including if you identify as CALD, Aboriginal or Torres Strait Islander. The information collected was necessary to enable us to assess eligibility for service, this may include presenting issues, referral points, support services.

An electronic account of client's situation, work undertaken, and outcomes are recorded on a secure archived data base.

Information collected in relation to Fundraising or Purchase payments

For the avoidance of doubt, fundraising refers to the activities undertaken by Lifeline South Coast to raise funds to support its services. This includes (but is not limited to), facilitating donations, sponsorships, workplace giving and fundraising campaigns.

When you make a donation, we collect your name and contact details, your credit card number, the card expiry date, and the amount donated. The only information that is required when you make a donation via our website is your credit card details.

Donors also have the availability to 'opt in' to providing other information such as date of birth, employment information, including but not limited to job title, opinions via surveys and questionnaires. This information can be provided to Lifeline South Coast in an 'opt in' basis, and donors may opt out of this at any time.

Purchases refers to payment for goods or services from Lifeline South Coast. This may include, but not limited to:

- Name and contact details, if consented
- Electronic registration and payment of training
- EFTPOS payment of goods in one of our shops or events

Information collected via Computer Program

Lifeline South Coast uses a computer program that uses personal information about individuals to perform its function.

However, it is used solely to assist human decision-making, and final decisions regarding communications, engagement, or program participation which are always made by authorised personnel.
These automated processes do not meet the materiality threshold of a decision that could reasonably be expected to significantly affect the rights or interests of an individual.

5.5.2 Collection Notices

Where Lifeline South Coast collects personal information from an individual in relation to fundraising, that individual should be provided with a collection notice.

Collection notices should generally be provided at the time the information is collected. Where this is not practical (for example, where information is collected from a third party), the collection notice should be provided at the time of first contact with the individual.

The collection notice should cover as many of the following matters as is reasonably practicable in the circumstances:

- Lifeline South Coast's name and contact details
- If the personal information was collected from a third-party source, how it was collected
- Where the personal information is required or authorised under an Australian law or a court/tribunal order – the fact that the collection is required / authorised
- The purposes for which the information is being collected
- The consequences to the individual of not providing the information
- To whom Lifeline South Coast usually discloses that kind of personal information
- Information about how to find or obtain our Privacy Policy, as well as information on access to and correction of personal information and how an individual may complain about a breach of the Australian Privacy Principles

- Whether we are likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

5.5.3 Direct Marketing

Lifeline South Coast may use individuals' personal information for direct marketing purposes, but only where:

- The direct marketing communication contains a prominent statement that the individual may opt out of receiving that type of communication, and
- The relevant individual has not made such a request.

5.5.4 Personal Information Collected from Third Parties

From time to time, we collect personal information from a third party or a publicly available source, only where the individual has consented to such collection or would reasonably expect us to collect their personal information in this way.

For example, we collect personal information:

- from referees provided by you in support of an application for a Lifeline South Coast position with us (either as an employee or as a contractor);
- from third parties such as contractors (including fundraising service providers) and list vendors;
- from other organisations that you have donated to, where you have consented to receiving information from like-minded organisations such as Lifeline Australia; and
- from academic and training organisations where required to verify a person's educational status.

We may also collect personal information about you from a third party during a person calling a Lifeline service such as the 13 11 14 telephone service. As we do not create records that identify people who use Lifeline services, personal information about you that is provided by another person in these circumstances, will not be contained in a record that is easily linked to you.

5.5.5 Unclear Consent

If personal information about an individual is collected from a third party and it is unclear that the individual has consented to the disclosure of their personal information to Lifeline South Coast, reasonable steps should be taken to contact the individual and ensure they are aware of the collection. In most cases, this can take place simultaneously with the first use of the information.

5.5.6 Unsolicited Information

If Lifeline South Coast receives personal information that was not solicited, and it is reasonable that we would not have collected the information in accordance with APP 3, we will destroy the information and ensure it is de-identified.

5.6 MINORS

In the delivery of crisis support services, Lifeline South Coast makes no active effort to collect personal information from children under the age of 18. However, Lifeline South Coast may collect personal information relating to children where the child has contacted that service and provides the information directly including on phone calls, or where another individual contacts Lifeline South Coast on behalf of the child with child safety concerns.

With specific reference to donations made to Lifeline South Coast:

In relation to donations, children who do wish to submit information to Lifeline South Coast (to process a donation) should secure permission from their parent or legal guardian prior to doing so.

5.7 COLLECTING INFORMATION VIA WEBSITES

Lifeline South Coast has its own public website — www.lifelinesouthcoast.org.au. There are several ways in which we collect information though our website.

Analytics
We use Google Analytics to collect data about your interaction with our website. The sole purpose of collecting your data in this way is to improve your experience when using our site.

The types of data we collect with these tools include:

- your device's IP address (collected and stored in an anonymized format);
- device screen size;
- device type, operating system and browser information;
- geographic location;
- referring domain and out link if applicable;
- search terms and pages visited; and
- date and time when website pages were accessed.

Cookies
Cookies are small data files transferred onto computers or devices by websites for recordkeeping purposes and to enhance functionality on the website.

Most browsers allow you to choose whether to accept cookies or not. If you do not wish to have cookies placed on your computer, please set your browser preferences to reject all cookies before accessing our website.

The core functionality on these platforms will be largely unaffected if you disable cookies in your browser but you may be unable to access some advanced functions.

Social Media
We use social media sites such as Facebook, Instagram, and LinkedIn to communicate with the public about Lifeline South Coast services. When you communicate with us using these social networking services we may collect your personal information, but we only use it to help us to communicate with you and the public.

Social media sites will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for Facebook, Instagram, and LinkedIn on their websites.

NB: Lifeline South Coast does not provide crisis support or suicide prevention services via Lifeline South Coast's social media platform (Facebook, Instagram, or LinkedIn).

5.8 DISCLOSURE

Lifeline South Coast does not disclose personal information to another person or organisation (including police, emergency services and other government agencies) unless one of the following applies:

- the individual has consented to the disclosure of their personal information;
- the individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, bodies or agencies and the disclosure:
    - in the case of personal information (that is not sensitive information) relates to the primary purpose for which it was collected; or in the case of sensitive information is directly related to the primary purpose for which it was collected; or
    - relates to collection from a third party outlined in this policy, that being a charitable or other likeminded organisation, including third party service providers who facilitate the sharing of information between such types of charitable or like-minded organisations; or
    - Contractors and service providers who perform services on our behalf, such as mailing houses, printers, information technology service providers, data matching and data washing service providers, database contractors and telemarketing agencies.
- the disclosure is otherwise required or authorised by law;
- we reasonably believe that the disclosure will prevent or lessen a serious and imminent threat to somebody's life, health or safety (including your own) or serious threat to public health, property or public safety;
- the individual has made threats to harm third parties;
- the individual has made threats against Lifeline South Coast personnel;
- the individual repeatedly makes nuisance contact including calls, chats or emails; or
- the disclosure is to a Lifeline South Coast service provider as described below.

From time to time, we may compile statistical data from the personal information we have collected. In these instances, the data will be aggregated and de-identified before it is disclosed to third parties.

5.9 QUALITY OF PERSONAL INFORMATION

To ensure that the personal information we collect is accurate, up-to-date, and complete we apply the following data quality processes:

- we record information in a consistent format through an IT system provided by Lifeline Australia that enables 13 11 14 and supports consistent recording;
- where necessary, confirm the accuracy of information we collect from a third party or a public source;
- promptly add updated or new personal information to existing records; and
- regularly audit our contact lists to check their accuracy.

We also review the quality of personal information before we use or disclose it. The way we apply the above data quality procedures depends on the nature of the personal information. For example:

- we do not create customer specific records (or records which are attributed to a specific person) for people who use Lifeline services such as the 13 11 14 telephone service and accordingly, have little reason to update personal information that may be included in such records;
- we do not, as a matter of standard practice, confirm the accuracy of personal information provided by a third-party using Lifeline services. We would only act on the information (irrespective of its quality) by disclosing it if we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to somebody's life, health or safety or serious threat to public health or public safety; and
- we keep employee specific employment and volunteer records and accordingly update those records to include new personal information.

5.10 STORAGE AND SECURITY OF INFORMATION

Lifeline South Coast takes steps to protect the personal information we hold against loss, unauthorised access, use, modification, or disclosure, and against other misuse.

These steps include:

- only allowing personnel with a 'need to know' to access our IT systems and records;
- password protection for accessing our electronic IT systems; and
- securing paper files in locked cabinets and physical access restrictions.

We may also store personal information electronically in the cloud.
When no longer required, personal information is destroyed, de-identified, or deleted in a secure manner.

5.11 ACCESS AND CORRECTION

Australian Privacy Principles (APPs) 12 and 13 give you the right to access personal information we hold about you and to request corrections to that personal information.

You may at any time request access to, or correction of, the personal information we hold about you. Lifeline South Coast will seek to respond to your request within 30 days.

A written request to access and/or correct your personal information should be addressed to the Privacy Officer and sent either via email to admin@llsc.org.au or via post to PO Box 404, Wollongong, NSW 2500.

If you ask for access to personal information that Lifeline Australia holds about you, individuals will be required to provide the following information before access or correction is undertaken:

- A written request for access and/or correction addressed to the Privacy Officer and sent either via email to secretariat@lifeline.org.au or via post to PO Box 173, Deakin West, ACT 2600.
- In order to enable Lifeline Australia to conduct a record search of our crisis support and suicide prevention service data bases we require you to provide us the following information:
- the date, time and number used to contact Lifeline's 13 11 14 service or Text4Good service; or
- the date, time and IP address used to access Lifeline's online crisis support chat service.
- Proof of identity (this may be achieved through a number of means, including using the 100-point identification system and proof of contact number, certified through a legal practitioner, pharmacist, police officer or GP with an accompanying statutory declaration).

Lifeline South Coast will not provide access to personal information unless we have verified that the person seeking access is the person to whom the information relates, or the law otherwise supports such access. In some cases, additional proof of identity information may be required, or access may have to be denied because ownership of a record cannot be proven.

If we refuse to give you access to, or correct, your personal information, we will notify you in writing setting out the reasons.

If we make a correction and we have disclosed the incorrect information to others, you can ask us to tell them about the correction. We must do so unless there is a valid reason not to.

If we refuse to correct your personal information, you can ask us to attach a statement which indicates that you believe the information is incorrect, and why.

5.12 NOTIFIABLE DATA BREACH

Under the Notifiable Data Breaches (NDB) scheme any organisation or agency the *Privacy Act 1988* covers must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

An organisation or agency must notify affected individuals and the OAIC about an eligible data breach.

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious harm to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.

An organisation or agency that suspects an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual.

If there are reasonable grounds to believe an eligible data breach has occurred, the organisation must promptly notify:

1. any individual at risk of serious harm,
2. the OAIC via the Notifiable Data Breach Form, and
3. Lifeline Australia within 48 hours

Details to report include:

- the organisation name and contact details
- a description of the data breach
- the kinds of information involved
- recommendations about the steps individuals should take in response to the data breach.

5.13 COMPLAINTS

If you wish to contact us about a privacy matter or are concerned about the way Lifeline South Coast have handled your personal information, you can lodge a written request or complaint with our Privacy Officer at either of the following addresses:

Postal Address: PO Box 404, Wollongong, NSW 2500; or
Email Address: admin@llsc.org.au

We will investigate any complaint and will notify you of our decision in relation to your complaint as soon as is practicable after it has been made (usually within 30 days).

If you are dissatisfied with our investigation of your concerns, you can lodge a complaint to the Office of the Australian Information Commissioner who is independent of Lifeline Australia.

6 Appendix A – Australian Privacy Principles

PART 1 – CONSIDERATION OF PERSONAL INFORMATION PRIVACY

1	1 Australian Privacy Principle 1—open and transparent management of personal information	
1.1	The object of this principle is to ensure that APP entities manage personal information in an open and transparent way	
COMPLIANCE WITH THE AUSTRALIAN PRIVACY PRINCIPLES ETC.		
1.2	An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that: (a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and (b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.	(a) Privacy Policy, & therefore APP review every at least 2 years to ensure operational compliance with up-to-date APP's. **(b)** Via LLSC Feedback & Complaints policy & procedure
APP PRIVACY POLICY		
1.3	An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity.	LLSC Privacy Policy reviewed & Board approved at ;east every 2 years.
1.4	Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information: (a) the kinds of personal information that the entity collects and holds; (b) how the entity collects and holds personal information; (c) the purposes for which the entity collects, holds, uses and discloses personal information;	(a) Section 4.4 (b) Sections 4.4 – 4.7 (c) Section 4.2 (d) Section 4.11 (e) Section 4.12

	(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information; (e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint; (f) whether the entity is likely to disclose personal information to overseas recipients; (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.	
AVAILABILITY OF APP PRIVACY POLICY ETC.		
1.5	An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available: (a) free of charge; and (b) in such form as is appropriate. Note: An APP entity will usually make its APP privacy policy available on the entity's website.	LLSC Privacy Policy is Disclosed on LLSC website
1.6	If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.	LLSC Privacy Policy is Disclosed on LLSC website, other forms actioned if requested. No request to date to note.

2	**Australian Privacy Principle 2—anonymity and pseudonymity**	
2.1	Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter	Section 4.1 Anonymous Interactions LLSC Privacy Policy outlines the purposes for collection of privacy data.
2.2	Subclause 2.1 does not apply if, in relation to that matter:	

	(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.	In registering for social media information individuals have the option of not identifying themselves. However, in certain circumstances Subclause 2.1(b) applies to LLSC, including: - employment / payroll, - accredited training

PART 2 – COLLECTION OF PERSONAL INFORMATION

3	**Australian Privacy Principle 3—collection of solicited personal information**	
PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION		
3.1	If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.	LLSC is not an agency as defined at B.8 of Australian Privacy Principles, Key Concepts
3.2	If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.	LLSC Privacy Policy outlines the purposes for collection of privacy data. Listed at section 4.
SENSITIVE INFORMATION		
3.3	An APP entity must not collect sensitive information about an individual unless: (a) the individual consents to the collection of the information and: (i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or	Consent is addressed at section 4.2 & 4.3.

	(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or (b) subclause 3.4 applies in relation to the information.	LLSC functions & activities for sensitive data collection are tabled at section 4.2
3.4	This subclause applies in relation to sensitive information about an individual if: (a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or (b) a permitted general situation exists in relation to the collection of the information by the APP entity; or (c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or (d) the APP entity is an enforcement body and the entity reasonably believes that: (i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or (ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or (e) the APP entity is a non-profit organisation and both of the following apply: (i) the information relates to the activities of the organisation; (ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities. Note: For *permitted general situation*, see section 16A. For *permitted health situation*, see section 16B.	LLSC mostly collects information where individuals voluntarily provide it. Sensitive information that may be collected from third parties is addressed at section 4.5.
MEANS OF COLLECTION		

3.5	An APP entity must collect personal information only by lawful and fair means.	Sensitive information that may be collected from third parties is addressed at section 4.5.
3.6	An APP entity must collect personal information about an individual only from the individual unless: (a) if the entity is an agency: (i) the individual consents to the collection of the information from someone other than the individual; or (ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or (b) it is unreasonable or impracticable to do so.	LLSC is not an agency as defined at B.8 of Australian Privacy Principles, Key Concepts. Sensitive information that may be collected from third parties is addressed at section 4.5.
SOLICITED PERSONAL INFORMAITON		
3.7	This principle applies to the collection of personal information that is solicited by an APP entity.	Noted above, the LLSC Privacy Policy outlines the purposes for collection of privacy data.

4	**Australian Privacy Principle 4—dealing with unsolicited personal information**	
4.1	If: (a) an APP entity receives personal information; and (b) the entity did not solicit the information; the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.	Policy section 4.5.2 outlines when LLSC must securely destroy unsolicited personal information.

4.2	The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.	
4.3	If: (a) the APP entity determines that the entity could not have collected the personal information; and (b) the information is not contained in a Commonwealth record; the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.	Policy section 4.5.2 outlines when LLSC must securely destroy unsolicited personal information.
4.4	If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.	

5	**Australian Privacy Principle 5—notification of the collection of personal information**	
5.1	At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances: (a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or (b) to otherwise ensure that the individual is aware of any such matters.	Section 4.4.2 Collection Notices
5.2	The matters for the purposes of subclause 5.1 are as follows: (a) the identity and contact details of the APP entity; (b) if: (i) the APP entity collects the personal information from someone other than the individual; or (ii) the individual may not be aware that the APP entity has collected the personal information;	All circumstances of APP 5.2 are specifically included in the Privacy Policy at section 4.4.2

	the fact that the entity so collects, or has collected, the information and the circumstances of that collection; (c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection); (d) the purposes for which the APP entity collects the personal information; (e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity; (f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity; (g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information; (h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint; (i) whether the APP entity is likely to disclose the personal information to overseas recipients; (j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.	

PART 3 – DEALING WITH PERSONAL INFORMATION

6	Use or disclosure of personal information	
USE OR DISCLOSURE		
6.1	If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: (a) the individual has consented to the use or disclosure of the information; or (b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information *Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.*	Policy section 4.2 Use for primary purpose and certain secondary purposes aligns with this.
6.2	This subclause applies in relation to the use or disclosure of personal information about an individual if: (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is: (i) if the information is sensitive information — directly related to the primary purpose; or (ii) if the information is not sensitive information — related to the primary purpose; or (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or (c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or (d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or (e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body	Policy section 4.2 and 4.2.1specify these subclauses

	Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.	
6.3	This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if: (a) the agency is not an enforcement body; and (b) the information is biometric information or biometric templates; and (c) the recipient of the information is an enforcement body; and (d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.	LLSC does not meet the definition of an Agency
6.4	If: (a) the APP entity is an organisation; and (b) subsection 16B(2) applied in relation to the collection of the personal information by the entity; the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.	Policy section 4.2.1 defines subsection 16B(2) of the *Privacy Act 1988*
WRITTEN NOTE OF USE OR DISCLOSURE		
6.5	If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.	CONNECT Documentation - case notes in the LLA system. Completed by the Crisis Supporter and the ISS when safety is at risk.
RELATED BODIES CORPORATE		
6.6	If: (a) an APP entity is a body corporate; and (b) the entity collects personal information from a related body corporate;	LLSC is not a body corporate

	this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.	
EXCEPTIONS		
6.7	This principle does not apply to the use or disclosure by an organisation of: (a) personal information for the purpose of direct marketing; or (b) government related identifiers.	

7	**Australian Privacy Principle 7—direct marketing**	
DIRECT MARKETING		
7.1	If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing. Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.	Policy section 4.4.3 Policy section 4.3 addresses consent for direct marketing and opt outs.
EXCEPTIONS – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION		
7.2	Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if: (a) the organisation collected the information from the individual; and (b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) the individual has not made such a request to the organisation.	Policy section 4.4.3

7.3	Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if: (a) the organisation collected the information from: (i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or (ii) someone other than the individual; and (b) either: (i) the individual has consented to the use or disclosure of the information for that purpose; or (ii) it is impracticable to obtain that consent; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) in each direct marketing communication with the individual: (i) the organisation includes a prominent statement that the individual may make such a request; or (ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and (e) the individual has not made such a request to the organisation.	Policy section 4.4.3 addresses direct marketing. Policy section 4.5 addresses personal information collected by third parties. Policy section 4.3 addresses consent for direct marketing and opt outs.
EXCEPTION – SENSITIVE INFORMATION		
7.4	Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.	Policy section 4.3 addresses consent for direct marketing and opt outs.
EXCEPTION – CONTRACTED SERVICE PROVIDERS		
7.5	Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:	N/A

	(a) the organisation is a contracted service provider for a Commonwealth contract; and (b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and (c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.	
INDIVIDUAL MAY REQUEST NOT TO RECEIVE DIRECT MARKETING COMMUNICATIONS ETC.		
7.6	If an organisation (the *first organisation*) uses or discloses personal information about an individual: (a) for the purpose of direct marketing by the first organisation; or (b) for the purpose of facilitating direct marketing by other organisations; the individual may: (c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and (d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and (e) request the first organisation to provide its source of the information.	This is addressed at Policy Section 4.3- Opting out of direct marketing
7.7	If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and: (a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and (b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.	This is addressed at Policy Section 4.3- Opting out of direct marketing
INTERACTION WITH OTHER LEGISLATION		
7.8	This principle does not apply to the extent that any of the following apply:	

	(aa) Division 5 of Part 7B of the Interactive Gambling Act 2001; (a) the Do Not Call Register Act 2006; (b) the Spam Act 2003; (c) any other Act of the Commonwealth, or a law in force in an external Territory, prescribed by the regulations.	

8	**Australian Privacy Principle 8—cross-border disclosure of personal information**	
8.1	Before an APP entity discloses personal information about an individual to a person (the *overseas recipient*): (a) who is not in Australia or an external Territory; and (b) who is not the entity or the individual; the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information. *Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.*	N/A - LLSC does not provide personal information to overseas recipients
8.2	Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if: (a) the entity reasonably believes that: (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or (b) both of the following apply:	N/A

	(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure; (ii) after being so informed, the individual consents to the disclosure; or (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or (f) the entity is an agency and both of the following apply: (i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; (ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body. *Note: For permitted general situation, see section 16A.*	

9	**Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers**	
ADOPTION OF GOVERNMENT RELATED IDENTIFIERS		
9.1	An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless: (a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or (b) subclause 9.3 applies in relation to the adoption.	N/A

	Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.	
USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS		
9.2	An organisation must not use or disclose a government related identifier of an individual unless: (a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or (b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or (c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or (e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or (f) subclause 9.3 applies in relation to the use or disclosure. Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A. Note 2: For *permitted general situation*, see section 16A.	N/A
REGULATIONS ABOUT ADOPTION, USE OR DISCLOSURE		
9.3	This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if: (a) the identifier is prescribed by the regulations; and	N/A

	(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and (c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations. Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).	

PART 4 – INTEGRITY OF PERSONAL INFORMATION

10	**Australian Privacy Principle 10—quality of personal information**	
10.1	An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.	The process applied at LLSC is outlines at section 4.9 of the policy
10.2	An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.	The process applied at LLSC is outlines at section 4.9 of the policy

11	**Australian Privacy Principle 11—security of personal information**	
11.1	If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure.	Policy section 4.10 – storage & security
11.2	If: (a) an APP entity holds personal information about an individual; and (b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and	Policy section 4.10 – storage & security addresses de-identification & disposal of personal information

	(c) the information is not contained in a Commonwealth record; and (d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information; the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.	

PART 5 – ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION

12	Australian Privacy Principle 12—access to personal information	
ACCESS		
12.1	If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.	Policy section 4.11 - Request in writing - 100pt identification
EXCEPTION TO ACCESS - AGENCY		
12.2	If: (a) the APP entity is an agency; and (b) the entity is required or authorised to refuse to give the individual access to the personal information by or under: (i) the Freedom of Information Act; or (ii) any other Act of the Commonwealth, or a law in force in an external Territory, that provides for access by persons to documents; then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.	N/A – LLSC does not meet the definition of an Agency
EXCEPTION TO ACCESS - ORGANISATION		
12.3	If the APP entity is an organisation, then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:	Policy section 4.11: LLSC will not provide access to personal information unless we have verified that the person

	(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or (b) giving access would have an unreasonable impact on the privacy of other individuals; or (c) the request for access is frivolous or vexatious; or (d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or (e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or (f) giving access would be unlawful; or (g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or (h) both of the following apply: (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or (i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or (j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.	seeking access is the person to whom the information relates, or the law otherwise supports such access.
DEALING WITH REQUESTS FOR ACCESS		

12.4	The APP entity must: (a) respond to the request for access to the personal information: (i) if the entity is an agency—within 30 days after the request is made; or (ii) if the entity is an organisation—within a reasonable period after the request is made; and (c) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so. (d)	Policy section 4.11 LLSC will seek to respond to your request within 30 days.
OTHER MEANS OF ACCESS		
12.5	If the APP entity refuses: (a) to give access to the personal information because of subclause 12.2 or 12.3; or (b) to give access in the manner requested by the individual; the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.	N/A – LLSC does not collect personal information that an individual would not have supplied themselves, or would easily have access to.
12.6	Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.	N/A
ACCESS CHARGES		
12.7	If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.	N/A – LLSC does not meet the definition of an Agency
12.8	If: (a) the APP entity is an organisation; and (b) the entity charges the individual for giving access to the personal information; the charge must not be excessive and must not apply to the making of the request.	LLSC does not charge individual to supply their personal information that may have been collected.
REFUSAL TO GIVE ACCESS		

12.9	If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out: (a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and (b) the mechanisms available to complain about the refusal; and (c) any other matter prescribed by the regulations.	Policy section 4.11
12.10	If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.	N/A

13	**Australian Privacy Principle 13—correction of personal information**	
CORRECTION		
13.1	If: (a) an APP entity holds personal information about an individual; and (b) either: (i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or (ii) the individual requests the entity to correct the information; the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.	Addressed at policy section 4.11

NOTIFICATION OF CORRECTION TO THIRD PARTIES		
13.2	If: (a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and (b) the individual requests the entity to notify the other APP entity of the correction; the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.	Addressed at policy section 4.11
REFUSAL TO CORRECT INFORMATION		
13.3	If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out: (a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and (b) the mechanisms available to complain about the refusal; and (c) any other matter prescribed by the regulations.	Policy section 4.11 If we refuse to correct your personal information, you can ask us to attach a statement which indicates that you believe the information is correct, and why.
REQUEST TO ASSOCIATE A STATEMENT		
13.4	If: (a) the APP entity refuses to correct the personal information as requested by the individual; and (b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;	Per above

	the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.	
DEALING WITH REQUESTS		
13.5	If a request is made under subclause 13.1 or 13.4, the APP entity: (a) must respond to the request: (i) if the entity is an agency—within 30 days after the request is made; or (ii) if the entity is an organisation—within a reasonable period after the request is made; and (b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).	Addressed at policy section 4.11