1. POLICY STATEMENT

Karingal St Laurence Limited (**genU**) and its related entities are required to comply with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

In situations where an individual's health information is protected by both Commonwealth and state based privacy principles, the Commonwealth APPs take precedence over the state legislation.

2. PURPOSE OF POLICY

The purpose of this policy is to:

- outline how genU collects, manages, and protects individuals' personal information to ensure compliance with all Commonwealth and state privacy legislation; and
- support genU's alignment with applicable compliance obligations, standards and frameworks required by genU's diverse programs and services.

3. SCOPE

This policy applies to genU meaning: Karingal St Laurence Limited and related bodies corporate, associations and trusts.

This policy applies to all workers and clients.

4. POLICY

4.1. Open and Transparent Management of Personal Information

genU will maintain a Privacy Policy and will provide this policy (or a version), to all workers and clients free and in an appropriate form. The policy is available at www.genu.org.au.

Enquiries or complaints about genU's Privacy Policy can be directed to the Privacy Officer via email: privacy@genu.org.au, via post: PO Box 558, Belmont VIC 3216 or via Tel: 1300 558 368

National Relay Service (NRS) for people who are deaf, hard of hearing or have a speech impairment:

TTY Users can phone 133677, then ask for 1300 558 368

Speak & Listen (speech-to-speech) Users can phone 1300 555 727, then ask for 1300 558 368

Internet Relay Users can connect to NRS on Helping you connect | Access Hub then ask for 1300 558 368.

Telephone Interpreter Service (TIS)

Please call 131 450 if you require a language interpreter to contact us.

4.2. Anonymity and Pseudonymity

When a client makes an initial inquiry about accessing genU goods and/or services, workers will give the client the opportunity of not identifying themselves, using a pseudonym or using a nickname, unless it is unlawful or impracticable to do so.

Once the client has commenced service, genU requires accurate personal information. However, if a client wishes to be identified by using a nickname or pseudonym whilst receiving goods and services, genU will give the client this opportunity, unless it is unlawful or impractical to do so.

4.3. Collection of Solicited Personal and Sensitive Information

genU only collects personal and sensitive information that is lawful and reasonably necessary for the delivery of requested goods and/or services. This may include, but is not limited to, an individual's contact details, date of birth, next of kin or emergency contact information, photograph, medical records, health information, and in some instances, limited financial information.

genU also collects personal information about workers relating to their employment. Personal information collected may include but is not limited to: name, date of birth, residency status, gender, tax file number, banking details, biometric information, superannuation details, qualifications, recruitment documentation e.g. referee reports, training attended and existing injury.

Where the collection of sensitive information is required, consent shall be confirmed at the point of collection unless the collection is required/authorised by law or is required to prevent or lessen a serious threat to an individual.

We will endeavour to collect information directly from the individual. Only in certain circumstances can information be collected from a third party (e.g. carer, nominee, or legal guardian) such as when an individual does not have capacity or is unable to provide necessary information required. In these circumstances it must be considered unreasonable or impracticable to obtain the information or consent directly from the individual concerned. Where this occurs, workers must make a written file note in the individual's file with the reason for seeking information from the third party and evidence of their legal authority.

4.4. Location Tracking

Location tracking applications may be used in cases where they support safety, scheduling or operational efficiency. The use of tracking must comply with relevant privacy legislation, including the Australian Privacy Principles (APPs).

Client addresses must never be disclosed via tracking apps or messaging platforms external to genU unless authorised. Location tracking data must never be used to monitor client locations, movements, or behaviours unless it forms part of an agreed support plan.

4.5. Dealing with Unsolicited Personal Information

On occasions, workers may receive unsolicited information about a client or another individual. When this occurs, genU will decide, within 14 calendar days, whether the information could have been obtained through standard operating practice. If genU forms the view that it could not, then the unsolicited personal information will be destroyed or the information de-identified.

Where unsolicited personal information would normally be destroyed as above, genU will not destroy and/or de-identify such information if it is considered there is a serious threat to health and safety of any individual or if the destruction or de-identification would contravene Australian law.

4.6. Notification of the Collection of Personal Information

We will take reasonable steps to ensure that the individual from whom the information is being obtained is aware of the following items, at or before the time of collection:

- genU, its address, and other contact details; and

- if any law requires the particular information to be collected; and
- the purpose for which the information is collected; and
- consequences (if any) for the individual if all or part of the information is not provided; and
- any third parties that genU usually discloses the information to; and
- genU's privacy policy and that it contains how to access and/or correct their own information; and
- how to make a privacy related complaint and how it will be dealt with; and
- whether any personal information will be disclosed to overseas recipients and which countries those recipients reside in (where practicable).

In the event that information is collected from a third party, the individual must be notified of the above information as soon as practicable.

4.7. Use of Personal Information

genU will only use an individual's personal information for the purpose that is collected, where it would be reasonably expected, or with the individual's consent. We may use personal information to: provide supports and services, assess the quality of, and make improvements to, our service delivery and to send communications about our services and events that may be of interest.

4.8. Disclosure of Personal Information

genU will only disclose personal information with consent from the individual. The only exceptions to this are where a permitted general situation exists including:

- where it is required to lessen or prevent a serious threat to life, health, or safety including when emergency or disaster declarations are in force; or
- taking appropriate action in relation to suspected unlawful activity or serious misconduct; or
- locating a person reported as missing; or
- where it is reasonably necessary for establishing, exercising, or defending a legal or equitable claim; or
- where it is reasonably necessary for matters of an enforcement body or the defence force in or outside of Australia; or
- conducting research; compiling or analysing statistics; management, funding or monitoring as part of the service agreement that genU has entered into; or
- where required as part of a mandatory reporting or disclosure eg: to child protection authorities
- when it is required or authorised by law, including under the Privacy Act.

When such personal information is disclosed under exception, without the individual's authorisation, a written file note must be included in the individual's file outlining the information disclosed, who it was disclosed to and the reasons for disclosure.

4.9. Direct Marketing

We may send communications to clients regarding services or events of genU if the communications could be reasonably expected, or where consent has been provided.

genU will not provide personal information to third parties for the purposes of direct marketing unless the individual has provided written consent or it is an obligation within a service contract that genU has entered into.

genU will never sell personal information.

On all direct marketing and event communication, genU will provide and draw attention to a simple method for individuals to opt out. A request to opt out of this type of communication will be actioned within a reasonable timeframe.

Within 14 days of request, genU will provide an individual with the source of their personal information used for direct marketing.

4.10. Cross-border Disclosure of Personal Information

genU will not disclose personal information about an individual to an interstate or overseas recipient unless:

- the individual is fully informed and has consented to the disclosure; or
- genU believes the recipient is subject to an information handling law or binding scheme providing substantially similar protections for an individual; or
- the recipient is party to an enforceable contract including adherence to the APPs and there is no reason to doubt the commitment; or
- the disclosure has been assessed by a legal representative of genU as allowable under the APP's or an applicable law.

4.11. Adoption, Use or Disclosure of Government Related or Unique Identifiers

genU will not adopt or use a government related identifier of an individual as its own identifier unless the adoption of the government related identifier is required or authorised by law or a court/tribunal order, or a condition of a government service agreement entered into by genU.

genU will not assign, adopt, or use a unique identifier unless necessary to facilitate the provision of services. Where the identifier has been assigned by another entity, and the use is not required under contract, genU will ensure that the correct permission or consent is secured prior to use.

4.12. Data Quality and Quality of Personal Information

genU will take all reasonable measures to ensure that an individual's information is up to date, complete and relevant. Records shown to be inaccurate or requiring updating will be amended and/or steps taken to update immediately.

4.13. Data Security and Security of Personal Information

genU will take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification, and/or disclosure.

Individuals' records (that may include personal, sensitive and health information) are stored securely and are accessible only to those who require the information.

Hard copy personal information will be stored securely and remain accessible only to genU.

Where genU no longer requires personal information, all reasonable steps to destroy or de-identify the information will be taken unless the information forms part of a state or Commonwealth record, or a requirement by or under law, or a court/tribunal order, to retain the information exists.

Our website collects data to enhance user experience. Data may include submissions, emails, and cookies for tracking. Cookies enhance website functionality and may be used for marketing purposes and website improvement. Where data is used by genU for marketing purposes, individuals will be given the option to opt out.

4.14. Use of Artificial Intelligence (AI) and Protection of Privacy

All use of AI involving personal information must undergo a due diligence process to ensure it is suitable for the intended use. This should include considering whether the product has been tested for such uses, how human oversight can be embedded into processes, the potential privacy and security risks, as well as who will have access to personal information input or generated by genU when using the product.

Regular reviews of the performance of AI must be conducted to ensure product remains fit for purpose, is appropriate and complies with privacy obligations.

AI tools including Chatbots must be clearly identified to the user. The use of AI decision making in a process must be disclosed to the individuals prior to use. Personal information must not be entered into publicly available generative AI tools.

4.15. Access to Personal Information

If genU holds personal information about an individual, genU will, on request, give the individual access to the information within a reasonable timeframe (typically within 30 calendar days or otherwise as prescribed by law) unless access is refused by law (as below).

An individual may request to access their information by contacting a senior staff member or the privacy officer. Requests that fall outside of the standard program processes must be sent to the privacy officer for review and response.

An individual may request their own information via an authorised third party such as a health provider, lawyer, or advocate. genU will ensure that authorisation from the individual is obtained prior to the release of any personal information to the third party.

Information should, where reasonable and practicable, be provided in a format suitable for the recipient.

genU may refuse access to an individual based on any of the following:

- giving access would pose a serious threat to life, health, or safety of any individual or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals; or
- the request for access is frivolous or vexatious; or
- the information requested relates to an existing or anticipated legal proceeding; or
- giving access would prejudice negotiations between the organisation and the individual; or
- giving access would be unlawful; or
- denying access is required or authorised by law or a court/tribunal order; or
- giving access would likely prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct; or
- giving access would be likely to prejudice an enforcement related activity conducted by, or on behalf of, an enforcement body; or

- giving access would reveal evaluative information in connection with a commercial sensitive decision-making process.

Any refusal to give access to personal information must be given in writing including the reason for the refusal and access to genU's complaints process.

4.16. Correction of Personal Information

At the request of an individual, genU will take all reasonable steps to correct personal information and ensure that it is accurate, up to date, complete, relevant, and not misleading.

When genU corrects personal information, it will:

- respond within 30 calendar days from the day after the day genU receives the request; and
- ensure the act of correction is recorded in the file and where practicable, who made the correction and the date of the correction; and
- notify other relevant third parties of the correction/change if it is required for the delivery of services; and
- if correction/change is refused genU will advise the individual in writing, the reason for refusal, the option to make an associated statement and the complaint process; and
- take reasonable steps to associate a statement with personal information it refuses to correct; and
- not charge an individual for making a request, correcting personal information, or associating a statement.

4.17. Transfer or closure of the practice of a health service provider

In the event of closure of any service provided by genU, notices and notification in accordance with relevant health privacy principles shall be adhered to.

4.18. Complaints

If an individual wishes to make a complaint in relation to privacy matters they can do so verbally, in writing (contact details provided on page 1 of this policy) or online https://www.genu.org.au/complaints-feedback-compliments/.

All complaints will be dealt with under the Disputes and Internal Complaints Procedure for Workers and the Complaints, Appeals and Feedback Foundational Policy & Procedure for all other matters.

If dissatisfied with the outcome, individuals may also wish to lodge a complaint through the Office of the Australian Information Commissioner (www.oaic.gov.au) or another regulatory body including those listed on our feedback page.

4.19. Notifiable Data Breach Scheme

genU is an organisation with obligations under the Privacy Act and required to comply with the Notifiable Data Breach scheme.

In the event of a data breach that meets the eligibility requirements, genU will provide notification to the Office of the Australian Information Commissioner, and the individuals whose information is involved. An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that genU holds
2. this is likely to result in serious harm to one or more individuals, and
3. genU has not been able to prevent the likely risk of serious harm with remedial action.

genU has developed a Data Breach Response Plan to assess any data breach; determine response and eligibility for notification to the commissioner and individuals.4.18 Assurance of Privacy

genU assesses the effectiveness of its privacy practices through conducting a variety of activities ensuring that personal information is handled in accordance with applicable legislation and this Policy.

Any serious breach of applicable Privacy legislation or this Policy will be escalated internally to Executive, CEO and reported to the board as outlined in the Data Breach Response Plan. The Privacy Act may also impose penalties in the form of monetary fines or in some cases imprisonment.

5. RESPONSIBILITY

Position	Responsibility
The Chair (or delegate) of the genU Board	Respond to any formal request where the CEO is the subject of a privacy complaint.
Chief Executive Officer (CEO) or their delegate	Promote and support implementation of the Privacy Policy. Oversee the investigation where a member of the Executive Team is the subject of a privacy complaint.
Chief Financial Officer	Approve the Privacy Policy, Data Breach Response Plan and associated documentation Support the effective implementation and monitoring and review of privacy across genU. Management and oversight to the Privacy Advisor/Officer
Chief Risk Officer	Convene the Data Breach Response Team Support incident response
Privacy Advisor/Officer	Respond to formal requests for information and managing complaints submitted in accordance with the Policy. Support and guide all business areas to adhere to this policy. Respond to all privacy breaches including data breaches where personal information is involved. Notify Office of the Australian Information Commissioner for any eligible data breaches.
Executive Team	Support workers to use record storage (management) systems and documentation within their divisions, departments or programs in a manner compliant with the provisions of the relevant legislation and this Policy. Ensure that people who perform duties on behalf of genU, including workers (includes volunteers), students, and contractors, undergo privacy compliance training.

Position	Responsibility
	Oversee investigation into privacy complaints made against any worker student, contractor within their division.
Senior Leadership Team / Managers / Team Leader	Support all workers and volunteers in complying with this policy. Report any privacy compliance concerns to Senior Management and the privacy advisor.
Workers	Comply with this policy and any other procedure that has privacy obligations. Promptly report any compliance concerns to their manager and/or the privacy advisor. Notify genU if there are any changes required to their own personal information. Ensure that all clients are aware of: • the Privacy Policy and where it can be obtained; and • the purposes for which genU collects, stores, and protects people's information and data; and • the need to provide accurate information including updating/correcting information; and • the consequences of not providing accurate information.
Clients	Notify genU if there are any changes to personal information required for the related goods/services.

6. RELATED DOCUMENTS

- Artificial Intelligence Policy
- Client Wellbeing, Rights and Responsibilities Foundational Policy
- Complaints and Appeals and Feedback Foundational Policy and Procedure
- Data Breach Response Plan
- Information Security Governance Framework Policy
- Organisational Compliance Policy
- Privacy Policy – Easy Read
- Risk Management Policy
- Records and Information Management Policy
- Supplier & Software Due Diligence Assessment Procedure

7. RELATED INTERNALTRAINING

- Privacy and Confidentiality at genU
- Code of Conduct
- Phishing Awareness
- Information Security Awareness Training

8. LEGISLATION & RELATED REFERENCES

- Federal privacy and related legislation including *Privacy Act 1988* (Cth), Privacy Regulation 2013 (Cth), *Social Security Act 1991* (Cth) and *Social Security (Administration) Act 1999 (*Cth)
- All applicable state-based privacy legislation including but not limited to: *Privacy and Data Protection Act 2014* (Vic); *Privacy and Personal Information Protection Act 1998* (NSW); Information Privacy Act 2009 (Qld); *Information Privacy Act 2014* (ACT); *Freedom of Information Act 1992* (WA); and *Personal Information Protection Act 2004* (Tas).
- All applicable state-based health privacy and records management legislation including but not limited to: *Health Records Act 2001* (Vic); *Health Care Act 2008 (*SA); *The Health Records and Information Privacy Act 2002* (NSW)
- Laws applicable to genU's regulated services including but not limited to: *National Disability Insurance Scheme Act 2013* (Cth) and all applicable state-based disability services laws (e.g. *Disability Act 2006* (Vic); *Social Services Regulation Act 2021* (Vic)); *Aged Care Act 1997* (Cth) and the *National Vocational Education and Training Regulator Act 2011* (Cth)

9. DEFINITIONS

Term	Definition
Australian Privacy Principles (APPs)	The legally binding principles expressed in the Privacy Act 1988 (Cth) that set out the standards, rights, and obligations in relation to handling, holding, accessing, and correcting personal information.
Client	A person or a group of people who are the end users of goods and/or services provided by genU or is directly affected by the services provided by genU and who receives, or relies on, or purchases one or more of genU goods and/or services. This definition is inclusive of people who use genU aged care service, retirement village residents, tenants, people with a disability, students, learners, and job seekers.
Individuals	Individuals include clients, workers, customers, any listed emergency contacts, guardians or support people relating to clients or workers that genU holds information about.
Personal Information	Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not.
Sensitive Information	A subset of personal information and includes information genU may collect such as racial or ethnic origin, political opinion, biometric information, religious beliefs, philosophical beliefs, sexual orientation or practices, transitional status/history, membership of a professional or trade association, criminal record, or health information.

Term	Definition
Data Breach	A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Eligible data breaches must be reported under the Notifiable Data Breach Scheme. An eligible data breach occurs these three criteria are satisfied: 1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the organisation holds 2. this is likely to result in serious harm to one or more individuals, and 3. the organisation has not been able to prevent the likely risk of serious harm with remedial action
Worker	A person engaged by genU in any capacity including: a director; an employee; supported employee; contractor/subcontractor; employee of a contractor/ subcontractor; consultant, employee of a labour hire company; an outworker, an apprentice or trainee; a work experience student; a student on placement or a volunteer.

10. RELATED RECORDS

Records must be maintained as per legal and contractual requirements. For guidance please refer to the Records and Information Management Policy and the Records Retention and Disposal Schedule.