Policy Statement	*Echuca Community for the Aged (ECA) ensures that personal information is collected, used, disclosed, and stored according to the relevant legislation, that is – the Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Privacy Amendment (Notifiable Data Breaches) Act 2017 and associated Privacy Regulations and Principles.*	
1. Legislation	1.1	The Privacy Act 1988[1], Privacy Amendment (*Enhancing Privacy Protection*) Act 2012[2] and the Privacy Amendment (*Notifiable Data Breaches*) Act 2017[3] regulate how we can collect, use, disclose and store personal information, and how individuals may access and correct personal information held about them.
	1.2	The Privacy Act defines personal information as *"Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".*
	1.3	The Australian Privacy Principles[4] (APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988 (Privacy Act). There are 13 Australian Privacy Principles 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
2. Who is responsible for upholding this policy	2.1	This policy applies to: ➢ ***ECA*** *– herein referred to as 'we' or 'us' or 'our'* ➢ Members of the Committee of Management ➢ Direct employees employed via an employment contract ➢ Indirect employees such as contractors, sub-contractors, students, trainees or unpaid volunteers of ECA.
3. Who we may collect information about	3.1	Information may be collected about a person or entity that: ➢ Uses our services for example, consumers, representatives, visitors ➢ Engages with with our services including employees, consumers and their representatives, contractors ➢ Visits our website
4. Who we may collect information from	4.1	Personal information (including sensitive information), may be collected from: ➢ a client or care recipient ➢ any person or organisation that assesses health status or care requirements, for example the Aged Care Assessment Team ➢ the health practitioner of a client or care recipient ➢ other health providers or facilities ➢ family members, a responsible person or significant persons of a client or care recipient ➢ a legal advisor of a client or care recipient
	4.2	We may collect personal information, including sensitive information: ➢ if an individual makes an enquiry regarding our services ➢ if an individual accesses our website ➢ during the recruitment process ➢ during provision of our services.; and ➢ during the discharge process.

[1] *Privacy Act* (1988) www.legislation.gov.au
[2] *Privacy Amendment (Enhancing Privacy Protection) Act* (2012) www.legislation.gov.au
[3] *Privacy Amendment (Notifiable Data Breaches) Act 2017* www.legislation.gov.au
[4] *Privacy Fact Sheet 17 – Australian Privacy Principles* (sourced April 2025), Office of the Australian Information Commissioner (OAIC) www.oaic.gov.au

5. Types of Information Collected	5.1	**Personal information** is any information that relates to an individual or any information from which an individual could become reasonably identifiable. ➢ This includes technical information obtained from a person's online behaviour which is unique to them. ➢ We may also need to collect personal information about other individuals related to the primary person (staff member, care recipient), such as family members.
	5.2	**Sensitive information** (a sub-set of personal information) includes information or an opinion about race or ethnic origin, political beliefs, religious beliefs or affiliations, sexual orientation, criminal record, health information, financial information including bank account details and genetic information. ➢ Due to the intimate nature of care and services provided, we do need to collect, use and store sensitive information to help us meet consumer care needs. ➢ When consumers accept care and services from us, it is implied that they accept that we may collect, use and store their sensitive information.
	5.3	**Government identifiers** such as Medicare, Pension or Veteran's Affairs numbers
	5.4	**Website information** obtained when a person visits our website including their internet protocol (IP) address, the date and time of their visit to our website, the pages they have accessed, the links on which they have clicked and the type of browser that they were using
	5.5	**Statistical data** - information relating to the use of our services for example demographics, data required under the National Quality Indicator Program. Refer further to policy 2.3.2 National Quality Indicator Program.
6. Quality information	6.1	We conduct internal quality activities that may involve using information about users of our services that we collect as part of care and service delivery.
	6.2	Quality activity information is primarily used for internal purposes, such as to identify trends, what we are doing well and opportunities for improvement.
	6.3	Generally, we consider that quality activity outcomes are beneficial to share in the wider aged care community. We do not report identifiable information such as individuals name or date of birth when sharing quality assurance activity outcomes.
7. How information is used	7.1	We will only use an individual's personal information in ways that a reasonable person would consider are fair and reasonable for a business of our type.
	7.2	For **care recipients**, we may use their personal information: ➢ to assess their application to receive our services ➢ in response to enquiries about our services ➢ to provide and manage the delivery of aged care services ➢ to enable allied health care providers and medical practitioners to provide care and services ➢ to obtain the correct level of government funding ➢ to complete quality, monitoring and assurance processes
	7.3	For the **nominated contact person** for a care recipient, information may be used: ➢ to provide updates in relation to health status, care or services being received ➢ to lawfully liaise with family if requested or needed ➢ to identify and inform them of any other services that may be of interest to them ➢ to improve our care and services (for example, directly or indirectly in improving quality or clinical outcomes, or in research which is in the public interest);
	7.4	For **staff or contractors**: ➢ to fulfil any of our legal requirements ➢ to assess an application for employment with us ➢ to provide and manage the delivery of our services ➢ to complete quality, monitoring and assurance processes ➢ to demonstrate legislative compliance for example, criminal history checks

8. Disclosing Information about a Care Recipient	8.1	We may disclose a care recipients' personal information to: ➢ Allied health professionals who assist us in providing care and services ➢ Medical practitioners ➢ Pharmacies ➢ External health agencies such as the ambulance service, hospitals ➢ The Australian Department of Social Services, ➢ The Aged Care Quality and Safety Commission, ➢ Medicare ➢ Relevant organisations or Government Departments
	8.2	We may not use or disclose personal information other than for the primary purpose of collection (as outlined above), unless: ➢ The secondary purpose is related to the primary purpose, and it would be reasonable to expect disclosure of the information for the secondary purpose; **OR** ➢ We believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety; **OR** ➢ The information is health information, and the collection, use or disclosure is necessary for research, the compilation or analysis of statistics, relevant to public health or public safety, it is impractical to obtain consent, the use or disclosure is conducted within the privacy principles and guidelines, and we reasonably believe that the recipient will not disclose the health information; **OR** ➢ We have reason to suspect unlawful activity and use or disclose the personal information as part of our investigation of the matter or in reporting our concerns to relevant persons or authorities; **OR** ➢ We reasonably believe that the use or disclosure is reasonably necessary to allow an enforcement body to enforce laws, protect the public revenue, prevent seriously improper conduct or prepare or conduct legal proceedings; **OR** ➢ The use or disclosure is otherwise required or authorised by law.
9. Security	9.1	All reasonable steps are taken to ensure that the personal information is protected against misuse, loss, unauthorised access, modification or disclosure.
	9.2	Personal information is held in both hard copy and electronic forms: ➢ in secure databases ➢ on secure premises and ➢ in secure cloud-based technology ➢ accessible only by authorised personnel.
	9.3	Non-current information is archived in secure premises in accordance with policy 2.7.2 Records Management.
	9.4	All organisation owned computers are password protected. Each staff member can access only the information relevant to the performance of their role**. Under no circumstance is a staff member to divulge their password to another person**.
	9.5	Staff and volunteers sign 2.9.1.5 Confidentiality Agreement on commencement to ensure they comply with their legislative responsibilities in relation to privacy and confidentiality.
	9.6	**Cloud based storage** - Some personal information is stored in secure cloud-based technology. Where information is stored in cloud-based technology operated by third party service providers, we take all reasonable steps to ensure that the third-party service provider adheres to Privacy Laws.
	9.7	**Transfer of data overseas**- All personal information is held in Australia. Our cloud-based storage systems are restricted from sharing personal information with overseas services or individuals.

10. Closed Circuit Television Surveillance (CCTV)	10.1	We use CCTV in the public areas at some of our residential aged care facility and other business premises to maintain the safety and security of care recipients, workers, visitors and all other people who enter our properties.
	10.2	Some CCTV systems may collect and store personal information. On rare occasions this information may be shared with law enforcement officers, or to comply with government regulation (such as in incident management).
	10.3	Refer also to policies 1.2.1 Personal Privacy and 2.2.3.10 Workplace Surveillance.
11. Employee Information	11.1	For regulatory and compliance reasons, we are required to keep records of current and past workers. These records are directly related to the employment relationship and are managed in accordance with workplace laws.
	11.2	Privacy laws may apply to employee personal information if the information is used for something that is not directly related to the employment relationship between the employer and employee.
	11.3	We maintain those records for a reasonable period, in accordance with policy 2.7.2 Records Management., after which the information may be deleted.
	11.4	**Work Candidates** – we may collect personal information from candidates and may store information about unsuccessful applicants for the purposes of future recruitment for a reasonable period, after which the information may be deleted.
	11.5	**Contractors, Volunteer and Student Records -** Personal information collected and held by us in relation to our contractors, volunteers and students will be managed in accordance with this policy and the Privacy Act.
12. Notification	12.1	This policy outlining our obligations in relation to Information Privacy is made available in the following formats: ➢ On our Website ➢ In the staff Handbook ➢ In the Consumer Handbook
	12.2	Staff have access to all policies and procedures through the organisational intranet.
13. Accessing Personal information	13.1	If an individual's personal information is held by the organisation, then we must, on written request by the individual, provide access to this information. The request must be made using 1.2.2.3 Request to Access Information form.
	13.2	A request for information can be declined under the following circumstances[5]: ➢ If we believe that giving access would pose a serious threat to the life, health or safety of an individual. ➢ Giving access would have an unreasonable impact on the privacy of others ➢ The request is seen to be vexatious or frivolous. ➢ The information relates to existing or anticipated legal proceedings and would not be accessible by the process of discovery in those proceedings. ➢ Giving access would reveal our intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations. ➢ Giving access would be unlawful. ➢ Denying access is required or authorised by under law or by court/tribunal order. ➢ We have reason to suspect unlawful activity or misconduct of a serious nature and giving access would be likely to prejudice action in that matter. ➢ Giving access would be likely to prejudice enforcement related activities conducted by an enforcement body. ➢ Giving access would compromise a commercially sensitive process.
	13.3	We must give access to the information in the manner requested by the individual within a reasonable period after the request is made. If access is refused, we must state the reasons and the mechanisms for complaint.

[5] *Privacy Fact Sheet 17 – Australian Privacy Principles* (sourced April 2025), Office of the Australian Information Commissioner (OAIC) www.oaic.gov.au

14. Requesting correction to personal information	14.1	We must take reasonable steps to ensure that personal information held is current, accurate and complete.
	14.2	Should a person believe that information held about them is incorrect, they can request this be amended using 1.2.2.3 Request to Access Information form.
	14.3	We must respond to the request within a 30 Days and must not charge individuals for making this correction.
	14.4	Should we refuse to amend or correct personal information about an individual, we must provide written reasons for the refusal, as well as relevant complaint mechanisms (*refer below to Part 15. Complaining about a Privacy Breach*)
15. Complaining about a Privacy Breach	15.1	The Executive Manager Clinical Care is the Privacy Officer.
	15.2	Any complaints made in relation to how we manage personal information should be made in the first instance to the Privacy Officer. This can be verbal or written.
	15.3	Should the complainant be dissatisfied with the outcome of their complaint, or if they have not received a response within 30 days, they can complain to the Office of the Australian Information Commissioner (OAIC) using the online Complaints Form[6]. This can be found at www.oaic.gov.au
	15.4	The OAIC has the power to investigate complaints made about privacy if it is clear there has been a breach in the Privacy Act 1988 and associated amendments and principles. The OAIC acts as an impartial regulator.
	15.5	Where a notifiable data breach has occurred, which is likely to result in serious harm, there are now clear guidelines in relation to the reporting of that breach (*refer below*).
16. Notifiable Data Breaches	16.1	As a Health Service Provider, and under the Privacy Amendment (*Notifiable Data Breaches*) Act 2017[7], we are obliged to report when a data breach has occurred, **which is likely to result in serious harm** to any individual whose personal information is involved in the breach.
	16.2	If there are reasonable grounds to believe there has been a data breach, then there is an obligation to notify the OAIC and the individuals whose data was affected with: ➢ our identity and contact details ➢ a description of what occurred/the data breach ➢ the kinds of information concerned; and ➢ the recommended next steps that individuals affected should take in response
	16.3	For notifiable breaches, and further resources about notifiable data breaches, an online notification form can be found at the OAIC website on www.oaic.gov.au or for more information, phone contact can be made with the OAIC on **1300 363 992**. Alternately, a statement can be prepared and submitted using a Word Document and provided to the Commissioner at: **Email**: enquiries@oaic.gov.au **Fax**: +61 2 9284 9666 **Post**: GPO Box 5218 Sydney NSW 2001
	16.4	An 'eligible data breach' arises when the following criteria are satisfied[8] – 1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information and; 2. This is likely to result in serious harm to one or more individuals and; 3. The service been unable to prevent the likely risk of harm with remedial action
	16.5	To determine whether an individual is at risk of serious harm consideration must be given to factors such as the sensitivity of the information, whether the information is protected by one or more security measures, the kind of person who could obtain the information and the nature of the harm.

[6] *Online Complaints Form*, Office of the Australian Information Commissioner (OAIC) www.oaic.gov.au
[7] *Privacy Amendment* (Notifiable Data Breaches) Act 2017 https://www.legislation.gov.au
[8] *Factsheet - Identifying eligible data breaches (sourced 2025)* at Office of the Australian Information Commissioner (OAIC) www.oaic.gov.au

17. The nature of Harm	17.1	In assessing the risk of serious harm, the organisation should consider the broad range of potential kinds of harm that may follow a data breach.
	17.2	It may be helpful when considering the likelihood of harm to consider a number of scenarios that may result in serious harm and the likelihood of each.
	17.3	Examples may include – ➢ Identify theft ➢ Significant financial loss ➢ Threats to an individual's physical safety ➢ Loss of business or employment opportunities ➢ Humiliation, damage to reputation or relationships ➢ Workplace or social bullying or marginalisation
18. Disclosure of information to overseas recipients	18.1	Where an overseas entity has requested personal information about a consumer or staff member, we must take care to ensure that, in providing this information, the overseas entity does not breach the Australian Privacy Principles[9].
	18.2	Where an overseas entity has requested personal information about a consumer or staff member, the individual to whom the information is related (or their nominated representative) must provide written consent for this information to be disclosed.
19. Exemptions from Privacy Laws	19.1	There are two situations in which a health or aged care service may use or share an individual's health information without consent. These are: 1. When a person's health or safety is seriously threatened and their health information will help - for example, if they are unconscious and the paramedics, doctors and nurses need to know if they are allergic to any medicines. 2. When the information will limit or prevent a serious threat to public health or safety: for example, if they have a severe contagious illness that the public should be warned about.
	19.2	Laws may differ by state, and there are certain exemptions that may apply in law enforcement situations and in a court of law.
Review	*This policy is reviewed every three years, or more frequently in response to identified risk, or where legislative or best-practice changes require amendment.*	

[9] *Privacy Fact Sheet 17 – Australian Privacy Principles* (sourced April 2025), Office of the Australian Information Commissioner (OAIC) www.oaic.gov.au