



Live Well
Home & Community Services



The Jesmond Group

Policies and Procedures



JG PRIVACY AND CONFIDENTIALITY POLICY

Purpose

The purpose of this policy is to outline how The Jesmond Group (TJG) collects, uses, stores, and discloses personal information, and how we protect the privacy and confidentiality of that information. By clearly communicating our personal information handling practices, we aim to give consumers, staff, volunteers, contractors, and other stakeholders a clear understanding of what information we collect and hold, why we collect it, and how we manage it. This policy also ensures everyone is aware of their rights to access or correct personal information and how we address privacy concerns.

Scope and Applicability

This Privacy & Confidentiality Policy applies to all TJG operations and services. It covers **all personal and health information** (in both digital and physical formats) that TJG collects, holds, or shares about individuals. This includes information about residents (older persons in our care), their families and representatives, staff, volunteers, contractors, and any other stakeholders associated with TJG. All TJG personnel, volunteers, and contractors are required to comply with this policy when handling personal information. We manage all personal information in accordance with applicable laws and best practices to protect privacy.

Older Person Outcome

Each older person (resident) receiving services from TJG can expect that their privacy is respected and personal information is kept confidential at all times. Individuals feel safe and respected, knowing that any personal details they share will be protected and only used to support their care and well-being. This outcome means our consumers, staff, volunteers, contractors, and other stakeholders maintain their dignity, trust in our services, and have confidence that their personal information is handled with utmost care and discretion.

Organisation Statement

TJG is firmly committed to upholding the privacy, dignity, and rights of every individual. We treat all personal information with respect and confidentiality as a core part of quality care. In the course of providing services and running our operations, we collect, use, and disclose personal and health information only as necessary and in line with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) and other relevant laws. We ensure that the behavior and interactions of our workforce do not compromise any individual's privacy.

All staff and volunteers are bound by confidentiality agreements and a Code of Conduct that requires them to keep personal information private. We provide training to our team on their privacy obligations and regularly reinforce these practices. Through these measures, TJG maintains a culture of privacy and confidentiality, and we manage personal information lawfully and responsibly.

Aged Care Standards

- Standard 1: The Individual
- Standard 2: The Organisation

1. Types of Information Collected and Held

We only collect and hold personal information that is reasonably necessary for our functions and activities. The types of information TJG may collect and maintain include:

- **Personal Details:** Name, date of birth, contact information (address, phone number, email), and other identifying details necessary to identify and care for the individual.
- **Health and Care Information:** Medical history, current health conditions, medications, treatment plans, assessments, and other health-related information required to provide appropriate care and services. Health information is considered sensitive and is handled with the highest degree of confidentiality.
- **Family and Representatives:** Contact details and relevant information about a consumer's primary or secondary contacts, emergency contacts, or legally authorized representatives (e.g. Power of Attorney or Guardian).
- **Financial and Billing Information:** Details required for funding or payment of services, such as Medicare or pension numbers, private health insurance details, billing addresses, and records of payments.
- **Social and Personal Preferences:** Information about the resident's background, cultural or religious needs, language preferences, dietary requirements, and personal likes/dislikes that help us tailor care to the individual. We may also record feedback or service preferences to improve the resident's experience.
- **Employee and Volunteer Information:** For TJG staff, volunteers, and contractors, we collect information relevant to their employment/engagement. This can include contact details, employment history, qualifications, emergency contact, and any required background checks (such as police checks or working-with-vulnerable-people checks). We also hold training records and other information needed to manage our workforce.

Please note: In this policy, "personal information" includes health information and sensitive information unless stated otherwise. Sensitive information (such as racial or ethnic origin, religious beliefs, or sexual orientation) is only collected if it is relevant to the person's care or employment and we have the individual's consent, or if required by law. We treat all sensitive personal data with extra care and security.

2. How Information is Collected and Held

Collection:

- We collect personal information directly from the individual wherever possible, usually with their knowledge and consent. For example, consumers (or their representatives) provide information via admission forms, healthcare assessments, face-to-face meetings, telephone calls, emails, and other communications. If the individual is unable to provide information (due to health or other reasons), or if we need additional details, we may collect information from a third party such as a family member, guardian, doctor, or a government agency (e.g. My Aged Care). We will only do this with the individual's consent or where it is authorized by law or otherwise *reasonable and necessary* (for instance, in an emergency or if the law requires it). We take steps to ensure individuals are aware when we collect personal information about them from someone else.

We are committed to collecting the minimum amount of information needed. Staff are instructed not to seek more information than necessary for providing quality care and services. If we receive personal information that we did not ask for and that is not needed (for example, **unsolicited information**), we will **securely destroy or de-identify it as soon as practicable**, provided it is lawful to do so.

Storage & Security:

- TJG holds personal information in a variety of forms, including paper records and electronic records. We have strong security measures in place to protect all personal information from loss, misuse, unauthorized access, or disclosure. These measures include:
 - **Physical Security:** Paper records and files are stored in secure, access-controlled locations. Personal documents are kept in locked filing cabinets or offices when not in use. We also implement on-site security measures (such as secure entry systems or surveillance in appropriate areas) to prevent unauthorized access to facilities where personal information is stored.
 - **Electronic Security:** Digital records are stored on secure computer systems and databases. All computers and devices containing personal information are password-protected, and we use up-to-date security software (such as firewalls, antivirus, and encryption where applicable) to safeguard our IT systems. Access to electronic records is restricted to staff members who need that information for their role, and each user is assigned secure login credentials. TJG also employs regular data backups and secure network protocols to protect electronic information.
 - **Access Controls and Confidentiality:** Only authorized personnel (care team members or administrative staff with a legitimate need) are permitted to access personal information. We educate our staff and volunteers about privacy and confidentiality, and every staff member signs a confidentiality agreement upon employment. This ensures they understand their obligation to keep information private. Any access to records is logged or monitored as appropriate under our systems.
 - **Retention and Disposal:** We retain personal information for as long as it is required to fulfill the purpose for which it was collected and to comply with legal requirements. When personal information is no longer needed, we dispose of it securely. Paper records are shredded or destroyed, and electronic files are securely deleted or anonymized. Secure

disposal procedures apply to both electronic and paper records, so that no personal data can be retrieved or reconstructed once discarded.

By using these collection practices and security safeguards, TJG ensures that personal information is handled in a safe and responsible manner throughout its life cycle, whether it is stored on-site, on our secure servers, or in transit between authorized recipients.

3. Purpose of the Information Collected & Held

TJG collects and holds personal information *only for purposes directly related to our care and services* or for other legitimate functions of our organization. In general, we use personal information to:

- **Provide Quality Care and Services:**
 - The primary purpose for collecting personal and health information is to deliver appropriate care and services to our consumers. This includes developing care plans, providing medical or personal care, tailoring services to individual needs, and making informed decisions in the best interest of each resident.
- **Administration and Operations:**
 - We use information for administrative tasks such as managing admissions, staff rostering, coordinating with healthcare providers, maintaining service records, and handling billing and financial processes. This ensures the smooth running of our facilities and that residents receive the services they require.
- **Communication:**
 - Contact information is used to communicate with stakeholders in a way that protects each resident's privacy and confidentiality in line with aged care and privacy laws. For residents, this includes contacting their nominated representatives about the person's well-being, general condition or changes in services, and only where there is appropriate consent or other lawful authority to do so.
 - For staff and contractors, personal details are used only to communicate employment-related information and are not disclosed to third parties without consent or another lawful basis.
- **Compliance with Legal and Regulatory Obligations:**
 - We collect and may disclose information as needed to meet obligations under Australian law. For instance, aged care providers must collect and provide certain data for government funding (such as Medicare or Centrelink details), report specific incidents, and comply with health regulations. We may be required to share information with government agencies or regulators (like the Department of Health or Aged Care Quality and Safety Commission) under the law or as part of audits and accreditation processes. Any such disclosures are done strictly in accordance with legal requirements.

3.1 Disclosure to Third Parties:

TJG treats all personal information as confidential. We do not disclose personal information to external individuals or organizations without consent, **unless an exception applies under the law**. The situations where we might share or disclose personal information include the following:

- **With Consent or at Request:**
 - We will share information with third parties (such as family members, friends, or other service providers) when the individual (or their legally authorized representative) has given consent or specifically requested us to do so.
- **Care Team and Medical Providers:**
 - We may disclose relevant personal and health information to doctors, specialists, pharmacists, pathology services, hospitals, or other healthcare professionals involved in a resident's care. This is done on a "need-to-know" basis to ensure continuity and quality of care, and wherever possible with the knowledge or consent of the resident or their representative.
- **Required or Authorized by Law:**
 - We may be required to disclose information if mandated by Australian law or a court/tribunal order. For example, we might need to provide information to law enforcement agencies under a warrant, or to report notifiable diseases or incidents to health authorities as required by legislation.
- **Serious Threats to Health or Safety:**
 - If we believe that disclosure is necessary to prevent or lessen a **serious or imminent threat** to someone's life, health or safety, or to public health or safety, we may share relevant information with an appropriate authority. For instance, in an emergency medical situation we might share information with hospital staff without prior consent, or we might alert authorities if someone is at risk of serious harm.
- **Suspected Unlawful Activity:**
 - If we have reason to suspect that unlawful activity (such as elder abuse, fraud, or a crime) has been, is being, or may be engaged in within our facility or services, we may disclose personal information as part of reporting it to the proper

authorities or taking required action. We will only do this in good faith and when permitted by law.

- **Other Permitted Situations:**

- The Privacy Act outlines certain *permitted general situations* and *permitted health situations* where personal information can be used or disclosed without consent (for example, for compassionate reasons or research under strict conditions). TJG will only rely on these exceptions in compliance with the law, and typically we will still seek consent where practical.

Outside of these circumstances, TJG will not disclose personal information to any third party without the individual's consent. In particular, we do not sell or exchange personal details for marketing purposes. We ensure that any third parties we work with (such as contracted service providers or consultants) are bound by confidentiality agreements or privacy laws so that they uphold the same standards of privacy as TJG. Our goal is to use personal information only to benefit the individual and to operate our services safely and legally.

3.2 Communication Guidance for Care Workers, RNs & Managers

Care workers and Registered Nurses (RNs), including Managers, have different responsibilities and levels of authority when sharing consumer information, and must always communicate within their defined scope of practice. The starting point is that staff only speak with nominated or legally authorised representatives and share the minimum information necessary for the purpose of the contact. Any employee who shares information outside their authority or scope of practice will be investigated and may be subject to disciplinary action under TJG's policies and procedures.

- **Care Staff - What they CAN provide**

Unregulated care workers/personal care assistants CAN usually only provide very limited, non-clinical information, and only to authorised contacts. Examples of what they can generally say:

- Very general condition (for example "resting comfortably", "up and about", "having lunch", "in their usual routine").
- Non-sensitive, day-to-day matters (for example "went on the bus outing today", "enjoyed sing-along activity this morning"), where the resident or client would reasonably expect this to be shared with their nominated contact.
- When speaking to visitors, unknown callers or people who are not nominated or legally authorised, care staff must:
 - Avoid confirming any identifying details about a resident or client (for example, not confirming that a person is in the service, their room number, diagnosis, or medications).
 - Politely decline and refer the enquiry to a registered nurse or manager, or advise that only the resident's nominated representative can receive information and offer to arrange a call-back.

- **Care staff – what they must NOT provide**

Care staff must not provide clinical or sensitive information, even to nominated representatives, unless it is clearly within their role and under direction from a registered nurse/manager. They must **NOT**:

- Discuss diagnoses, prognosis, changes to complex care plans, medication changes, incidents, behavioural assessments or restraint, or any test results.
- Disclose information about other residents/clients, staff, or internal investigations/incident reports, or provide copies of records.
- Email, text or share photos, videos or written information about residents from personal devices, or disclose information on social media, to any person.

- **Registered Nurses/Managers – what they CAN provide**

Registered nurses (RNs) and Managers are the appropriate people to provide more detailed updates to nominated or legally authorised representatives, in line with privacy law and professional standards. Subject to consent or other lawful authority, they may:

- Provide clinical updates in plain language (for example changes in health status, new or changed medications, recent falls, hospital transfers, wound status, or behaviour and psychological symptoms of dementia management).
- Discuss care plans, risk management strategies, upcoming assessments or case conferences, and decisions about treatment or services.
- RNs/managers are also the appropriate contacts to speak with external professionals (for example GPs, allied health, specialists) about the consumer care, consistent with privacy and health records obligations.

- **Registered Nurses/Managers - LIMITS on what they provide**

Even RNs and Managers **must still follow the "minimum necessary" and "need to know" principles**. They must **NOT**:

- Share any resident/client information with callers or visitors who are not verified as nominated or legally authorised, beyond very general, non-identifying comments such as "we will ask the resident or their representative to contact you".

- Disclose information about other residents/clients, staff, or internal investigations/incident reports, or provide copies of records without following the organisation's access-to-records and privacy procedures.

4. Accessing Personal Information

Individuals have the right to access the personal information that TJG holds about them, in accordance with Australian Privacy Principle 12. This means a resident, client, staff member, or other person whose information we hold can request to see or obtain a copy of their own personal information.

4.1 How to Request Access:

- To access your personal information, you can send a request to us (*preferably in writing*) addressed to the TJG Privacy Officer. You may use email (see contact details in the "General Enquiry" section) or a written letter. Please describe the information you wish to access, and provide your contact details. For security reasons, we will need to verify your identity before granting access to ensure that we are releasing information to the correct person. For example, we might ask you to provide identification or, if you are a representative, proof of your authority to act on behalf of the individual.

Our Response:

- Once we receive an access request and verify identity, we will respond within a reasonable timeframe. We aim to reply to access requests as quickly as possible, typically within 14 days. If the request is straightforward, we may be able to provide the information sooner. We will either provide the requested information or, if we need to refuse access to some or all of the information, we will inform you in writing of the reasons for refusal. In rare cases, we might lawfully refuse access or only give partial access, for example if:
 - Giving access would pose a serious threat to the life, health or safety of anyone, or to public health or safety;
 - Providing the information would have an unreasonable impact on someone else's privacy;
 - The request is frivolous or vexatious;
 - The information relates to anticipated or actual legal proceedings and would not be accessible via those proceedings;
 - Giving access would reveal our intentions in negotiations with you in a way that prejudices those negotiations;
 - Giving access would be unlawful, or denying access is required or authorized by law;
 - Or if the information is held under a law enforcing agency's request (e.g., we are ordered not to disclose it).

If we refuse access to any part of your request, our written notice will explain the reasons (except where it would be unreasonable to do so) and outline any steps available to you to challenge our decision.

4.2 Access Arrangements and Fees:

- We will work with you to provide access in the way that suits you best (for example, providing copies of documents, or a summary of the information, or allowing you to view the records in person) provided it's reasonable and practical. There is no fee to make a request, however we may charge a **small fee for the administrative cost** of providing access (for example, photocopying or postage), but any such charge **will not be excessive and we will inform you of any cost before proceeding**. We do not charge any fee for simply lodging a request. Our priority is to enable you to access your information without barriers usually **2 to 4 weeks from request**.

4.3 Seeking Correction of Personal Information

We are committed to ensuring that the personal information we hold is **accurate, complete, up-to-date, relevant, and not misleading**. If you believe any information we have about you is incorrect or out of date, you have the right to request a correction.

How to Request a Correction:

- To correct your personal information, please contact the TJG Privacy Officer (see contact details below) with details of the information to be corrected and the updated information. You can make this request in writing (by email or letter). We may ask for some verification or documentation depending on the change (for example, if you need to correct your name or date of birth, we might request proof of the correct details).

Our Response: When we receive a correction request, we will:

- Take reasonable steps to verify the accuracy of the new information and then **correct your records as soon as practicable** if we agree the information is wrong. This includes updating any third parties or systems that need the corrected data.
- If we disagree that the information is inaccurate or if we are unable to amend the record for some reason, we will let you know our reasons. In such cases, you have the right to request that we attach a statement to the record indicating that you believe the information is inaccurate or out-of-date, so future users of the record are aware of the dispute.

If we cannot fulfill your request to correct information, we will provide you with a written notice stating the reasons for refusal and how you can complain about our decision. We will also inform you about any further steps you can take, such as having a statement added to your file or contacting the relevant authorities. Our goal is to resolve any accuracy issues to your satisfaction wherever possible.

We do not charge any fees for correcting personal information. We encourage all individuals to keep us informed of any changes to their personal details (for example, change of address or contact number) so we can maintain accurate records.

5. Consumer Access to Jesmond Group Policies and Procedures

The Jesmond Group (TJG) recognises the importance of transparency and building trust with consumers, families, and other stakeholders. While there is **no legal requirement under Australian law** for TJG to disclose internal policies and procedures to consumers or the public other than our workforce, we acknowledge that access to certain documents—such as this **Privacy & Confidentiality Policy**—may assist in promoting understanding, confidence, and accountability.

As such:

- **TJG will make selected policies available** upon request, particularly those that directly impact consumer rights, care, or service provision.
 - Examples of such policies may include: the Privacy & Confidentiality Policy, Complaints Handling Policy, Code of Conduct, or Service Charter.
- **Internal operational procedures**, staff management protocols, and other governance documents that do not directly affect consumer rights or care services will generally **not be provided**, as they are considered confidential internal documents.

Any requests for access to policies should be directed to our Privacy Officer. TJG will consider each request on a case-by-case basis and respond appropriately, balancing transparency with our obligations to maintain operational confidentiality and security.

6. Complaints about a Breach in the APPs

TJG takes privacy and confidentiality very seriously. If you believe that we have not handled your personal information in accordance with this policy or breached our obligations under the Australian Privacy Principles, you have the right to make a complaint. We view complaints as an opportunity to resolve issues and improve our processes.

6.1 How to Lodge a Privacy Complaint:

- You can make a complaint by contacting the TJG **Privacy Officer** via the contact details provided in the "General Enquiry" section below. Please outline the nature of your complaint – for example, what happened, what personal information or interaction it involves, and what you believe has been breached. It is best to put your complaint in writing (via email or letter) so that the details are clear, but you may also call us if you prefer. All privacy complaints will be handled **confidentially and promptly**.
- **Our Complaint Handling Process:**
 - Once we receive your complaint, we will acknowledge it and begin an investigation. The Privacy Officer will review the issue, which may involve speaking with the people involved or examining relevant records. We aim to respond with the outcome of our investigation and any actions we will take to resolve the issue in a timely manner. You can expect a response or update usually within 30 days or sooner. We will let you know what we found and what we will do to address any problem. If a mistake was made, we will take steps to fix it and to prevent it from happening again. **We do not charge any fees to handle privacy complaints.**
- **If You Are Not Satisfied:**
 - We hope to resolve all complaints internally, but if you are not satisfied with our response or the outcome, you have further options. You can escalate the matter to the **Office of the Australian Information Commissioner (OAIC)**, which is the independent regulator for privacy in Australia. The OAIC can review privacy complaints and may investigate or conciliate the matter. We will provide you with information on how to contact the OAIC in our response to your complaint.

Alternatively, you may directly contact the OAIC for advice or to lodge a complaint. The OAIC can be reached by calling **1300 363 992** (the OAIC Privacy Hotline) or by visiting their website at ****www.oaic.gov.au****. The OAIC's website provides an online complaint form and further guidance on what to include in a privacy complaint. There is no charge to lodge a complaint with the OAIC.

For Older Persons receiving aged care services, you also have the right to raise concerns with the **Aged Care Quality and Safety Commission**, by calling 1800 951 822 or by visiting the website at ****www.agedcarequality.gov.au**** especially if the issue relates to how your personal information affects the quality of your care. However, for pure privacy issues, the OAIC is the specialist body. **We encourage you to allow us the chance to address your concerns first**, but you are free to approach these external agencies at any time. TJG will cooperate fully with any external investigation by the OAIC or other relevant authority and will abide by their findings and recommendations to resolve the complaint.

7. Enquiries

For any **enquiries** about this Privacy & Confidentiality Policy or how we handle personal information at The Jesmond Group, please contact our Privacy Officer. We welcome questions, feedback, and requests for additional information. You can reach the Privacy Officer at:

- Email: qualitycompliance@jesmondgroup.com.au
- Address: The Jesmond Group, Level 2, Suite 2, 9 George Street, North Strathfield, NSW 2136
- Phone: 1300 537 663

If you have special requirements (for example, you need an interpreter or assistance due to hearing impairment), we can facilitate appropriate support to communicate with you. Please let us know and we will arrange the Translating and Interpreting Service or National Relay Service as needed.

This Privacy & Confidentiality Policy will be provided to anyone who requests it. It is also included in resident information packs and is available to staff and stakeholders. We regularly review this policy to ensure it remains up-to-date with current laws and best practices.

Key Definitions

Term or Abbreviation	Definition
Privacy	Privacy is the right of individuals to have their personal information handled in a way that is consistent with their expectations, and protected from misuse, loss, or unauthorised access.
Confidentiality	Confidentiality refers to the obligation to keep a person's information private and not disclose it without consent, unless required or authorised by law.
Personal Information	Any information or opinion about an identified individual, or an individual who is reasonably identifiable. This includes names, addresses, contact details, and sensitive information (see below), whether true or not, and whether recorded in a material form or not. (Defined under the Privacy Act 1988 (Cth)).
Sensitive Information	A subset of personal information that includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation or practices, criminal record, or health information. Sensitive information has higher protection under law. (Defined under s6 of the Privacy Act 1988 (Cth)).
Health Information	A type of sensitive information that relates to an individual's physical or mental health or disability, expressed wishes about future health care, health services provided, or personal information collected to provide a health service. (Defined under the Privacy Act 1988 and the Health Records and Information Privacy Act 2002 (NSW)).
Australian Privacy Principles (APPs)	A set of 13 legally binding principles under the <i>Privacy Act 1988 (Cth)</i> that govern standards, rights and obligations around the collection, use and disclosure, and secure management of personal information. APPs apply to most Australian government agencies and many private sector organisations.
The Privacy Act 1988 (Cth)	The primary Australian law that regulates the handling of personal information by Australian Government agencies and some private sector organisations. It includes the Australian Privacy Principles and regulates the collection, use, storage, and disclosure of personal and sensitive information.
Notifiable Data Breach (NDB) Scheme	A legal requirement under the Privacy Act 1988 (Cth) that requires organisations to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals when a data breach is likely to result in serious harm.
Consent	Permission given voluntarily, informed and current, either in writing, verbally, or implied, for the collection, use or disclosure of personal or sensitive information. Consent must be specific to the activity and able to be withdrawn at any time.
De-identified Information	Personal information that has been stripped of identifying details so that the individual is no longer reasonably identifiable. De-identified information is not subject to the APPs.
APP Entity	An organisation or agency that is subject to the <i>Privacy Act 1988 (Cth)</i> and must comply with the Australian Privacy Principles. This includes aged care providers like The Jesmond Group.
Representative/ Person Responsible	An individual legally authorised to act on behalf of another person, such as a Guardian, Enduring Power of Attorney, or under the Hierarchy of Persons Responsible, especially in decisions regarding care, health, or access to personal information.
Disclosure	When personal information is made accessible to others outside the organisation, even if it is not directly handed over. Disclosure must be done in accordance with the APPs and usually with consent, unless an exemption applies (e.g. serious threat to life or required by law).
Use	The handling of personal information within the organisation, including the analysis, application, or reference to information in decision-making or service delivery.
Office of the Australian Information Commissioner (OAIC)	An independent national regulator for privacy and freedom of information. The OAIC handles privacy complaints, conducts investigations, and promotes best practices in information handling.
Internal Document	Any policy, procedure, or protocol used within an organisation to manage operations, staff, or service delivery. Internal documents are typically not public unless required by law or disclosed by the organisation for transparency.
Older Person / Older People / Consumers / Residents/ Clients	"Older people and consumers including residents and clients" refer to individuals receiving aged care services, including Aboriginal and Torres Strait Islander (ATSI) peoples and those from Culturally and Linguistically Diverse (CALD) backgrounds. This inclusive definition ensures that the diverse needs,

preferences, and identities of all individuals are recognised and met within aged care services. While 'older people' generally refers to those advanced in age, specific eligibility criteria vary across services.

Relevant Legislation

- [Aged Care Act 2024](#)
- [Aged Care Rules 2025](#)
- [Code of Conduct for Aged Care](#)
- [Australian Privacy Principles \(APPs\)](#)
- [Notifiable Data Breaches \(NDB\) Scheme](#)
- [Office of the Australian Information Commissioner \(OAIC\)](#)
- [Strengthened Aged Care Quality Standards](#)
- [Privacy Act 1988](#)

Relevant Policies

- This policy is applicable across all policies within TJG

Relevant Procedures

- This policy is applicable across all procedures within TJG

Related Documents

- This policy is applicable across all documents within TJG

Key Words for Search

Privacy	Confidentiality	Information Breach	Privacy Officer
Data Breach			

Review History

Date of Update	Outline of Change
19 February 2019	• Created • SMEs: ◦ Operational Manager
22 September 2021	• Reviewed with minor revisions.
19 December 2024	• Reviewed with no revisions
15 May 2025	• Reviewed with major changes to include legislative changes and information related to internal documents.
30 October 2025	• Minor update to include contemporary references from ACQSC and Aged Care Rules 2025.

Version Control

Approver	Owner	Date Approved	Document Expiry Date
Chief Operating Officer	Operations	1 July 2025	30 June 2028

Previous

« [JG Partnered Care and Referral Pathways Policy](#)

Next

[JG Promoting Older Persons and Consumer Mental Health and Wellbeing Policy](#) »