ACN 637 232 752

OM8
Information Management

Thrive Care Group Subsidiaries

This policy is part of Thrive Care Group's (Thrive) comprehensive policy suite, designed to guide and govern operations across all subsidiaries. It establishes a unified framework that ensures consistent standards, accountability, and alignment with Thrive core values and strategic objectives. The policy applies to all employees, contractors, and stakeholders within Thrive and its subsidiaries, supporting seamless governance and compliance throughout the organisation.

OM8 Information Management

Policy Statement

1. Thrive is committed to managing Information in a way that supports ethical practice, legal compliance, and high-quality service delivery. This policy outlines how Information is created, stored, accessed, shared, and protected across the organisation. It applies to all team members and board members.

2. Information management at Thrive supports person centred practice, ensures privacy and confidentiality, and enables effective decision-making. It contributes to compliance with the *Privacy Act 1988 (Cth)*, Aged Care Quality Standards, and National Disability Insurance Scheme (NDIS) Practice Standards.

3. Thrive manages two types of Information: Personal Information and Organisational Information. This policy outlines how both are handled to ensure security, accuracy, and accessibility.

Procedures

1. Information Management Framework

    a. Thrive considers people, processes, technology, content, and Information life cycles to ensure Information is effectively managed.

    b. Information management supports timely and relevant decisions, reduces duplication, and ensures compliance with laws, regulations, policies, and accreditation requirements.

    c. Thrive's framework covers:

        i. Description
        ii. Ownership
        iii. Security
        iv. Compliance
        v. Sharing
        vi. Quality and records

2. Ownership

   Thrive will:

   a. Protect intellectual property rights and enforce copyright.

   b. Ensure team members respect copyright owned by others.

   Team members will:

   a. Understand their responsibilities for documents and records including classification, retention and disposal.

   b. Maintain an up-to-date list of authorised custodians.

   c. Return all information assets upon termination of employment.

3. Accuracy and Access

   Thrive will:

   a. Ensure Information is accurate and complete at the time of collection.

   b. Correct errors where reasonable and inform clients if changes are not possible.

   c. Refer clients to the Privacy and Confidentiality Policy for access to records.

4. Storage and Security

   Thrive will:

   a. Store most Information electronically to improve accessibility.

   b. Apply the same responsibilities to paper files where required.

   c. Restrict access to confidential documents to authorised team members.

   d. Preserve Information with long-term or historical value.

5. Information Coordination

   Thrive will:

   a. Share and re-use Information subject to legal and policy requirements.

   b. Avoid redundancy by organising Information for visibility and re-use (e.g. shared drives, naming conventions).

c. Share Information externally via the website, newsletters, emails and forums.

d. Maintain records of external meetings and conferences.

e. Share relevant information internally through roadshows, meetings and emails.

6. Quality and Records

   Thrive will:

   a. Distinguish high-value Information from transient content.

   b. Require team members to consult managers before sharing sensitive Information.

   c. Ensure records are authentic, reliable and usable.

   d. Manage records throughout their life cycle.

7. Client Information

   Thrive will:

   a. Collect and provide information through various communication methods.

   b. Record all client-related Information in the relevant client file.

   c. Collect data on cultural background, health, legal status and quality of life.

   d. Align data collection with national and state standards.

   e. Use de-identified data for reporting and ensure client awareness and consent.

8. Privacy and Confidentiality

   Thrive will:

   a. Collect personal information only for organisational purposes.

   b. Inform clients about the purpose, use and disclosure of their information.

   c. Use personal information only for its intended purpose or with consent.

   d. Ensure data quality through regular updates and verification.

   e. Protect data using physical, technical and administrative safeguards.

   f. Provide access to personal information unless legally exempt.

g. Respond to access or amendment requests within 45 days.

h. Allow anonymity where lawful and practicable.

i. Avoid adopting government-issued identifiers as internal codes.

9. Confidential Information

Thrive will:

a. Treat non-public Information as confidential.

b. Require team members to consult managers before sharing sensitive Information.

c. Ensure all team members adhere to the Code of Conduct.

d. Protect stakeholder information in line with contractual agreements.

10. Breach of Privacy and Confidentiality

Thrive will:

a. Encourage team members to report concerns to their supervisor.

b. Investigate breaches and apply disciplinary action where appropriate.

c. Provide clients and stakeholders with accessible complaint mechanisms.

11. Information Technology

Thrive will:

a. Provide secure access to ICT systems during induction.

b. Remove access when no longer required.

c. Restrict access to authorised users only.

d. Store data on secure servers with appropriate access controls.

e. Prohibit storage of Confidential Information on local devices.

f. Require permission for data sharing or downloading.

12. Mobile Resources

    Thrive will:

    a. Enable security features to mobile devices if issued.

    b. Hold users accountable for appropriate use.

13. Email and Viruses

    Thrive will:

    a. Use filtering services to block spam and malicious content.

    b. Require team members to report suspicious emails to the Head of Information Technology.

    c. Maintain up-to-date antivirus protection.

14. Employee Files

    Thrive will:

    a. Restrict access to team member files to authorised personnel.

    b. Archive digital files after 10 years and destroy them thereafter.

    c. Allow team members to access their files through the People & Culture team.

15. Internal Auditing of Information Management

    Thrive will:

    a. Complete an annual internal audit of information managed across Thrive. The audit must assess compliance with this policy, relevant legislation and organisational requirements. The audit supports accountability, transparency and continuous improvement.

    b. Review Information for accuracy, completeness and currency. This includes reviewing assessment reports, treatment plans, progress notes, communications, and all required documents or records retained in client and organisational files.

    c. Confirm that required documents are maintained within each file, including agreements, support plans, consent records and schedules of support, where relevant. Document any discrepancies or missing Information and ensure corrective action is completed.

d. Complete internal audits on a periodic or rolling basis, ensuring that all relevant records have undergone review within the required timeframe. Add a notation to the record (e.g. case management note or internal log entry) confirming that the internal audit has been completed.

e. Review employee files annually on each team member's work anniversary to ensure compliance with record-keeping requirements. When a file is reviewed, add a management note acknowledging the internal audit.

f. Review all policies, procedures, governance documents and committee terms of reference at least every two years to maintain alignment with legislative requirements, organisational objectives and best practice. Update the version and date of review, and record all changes made.

g. Ensure that the outcomes of internal audits inform continuous improvement activities and support Thrive's commitment to ethical practice, legal compliance, and high-quality Information Management.

Related Business Procedures

1. OM1 – Governing Body Policy
2. OM2 – Delegations Policy
3. OM3 – Organisational Risk Management Policy
4. OM6 – Incident Management Policy

Responsible Persons

1. The Chief Executive Officer must:

    a. Manage and monitor compliance with this policy.

    h. Support team member competence and compliance with this policy.

    i. Lead Information Management Systems and reviews.

    j. Ensure systems protect privacy and Confidentiality.

2. Management must:

    a. Manage and monitor compliance with this policy.

    b. Ensure team members receive appropriate training, supervision and debriefing to comply with this policy.

3. All Thrive team members must comply with this policy.

Definitions

1. **Audit**: A process used to assess compliance with policies, procedures, regulatory obligations and organisational standards. Audits include the review of records, documents, systems and practices to confirm accuracy, completeness and alignment with required standards.

2. **Board**: The legally responsible managing body of Thrive.

3. **Board Member**: A Board member who does not have a formal title, such as Chair, Vice Chair, Treasurer or Secretary.

4. **Confidential Information**: Any Information not in the Public Domain that is disclosed in confidence.

5. **Confidentiality**: The obligation to keep Information private and protect it throughout its lifecycle.

6. **Consent**: Voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.

7. **De-identified Data**: Data that has been stripped of Personal Information so that individuals cannot be identified

8. **Document**: Any of the forms in which Information is carried.

9. **ICT**: Information and Communication Technology.

10. **Individual**: Any person such as a client, staff member, Board Member, volunteer, student, contractor or a member of the public.

11. **Information**: Codified knowledge which is transferred and stored in various formats.

12. **Information Management System**: The systematic process of managing Information to ensure accuracy, accessibility and security.

13. **Management**: Thrive's executive and leadership team responsible for overseeing its operations, strategic planning, and decision-making processes.

14. **Manager**: An individual responsible for overseeing operations and staff.

15. **Organisational Information:** Information about Thrive that may be public or confidential.

16. **People Manager**: An individual responsible for leading and managing a team.

17. **Personal Information**: Information or opinion about an Individual, guided by the *Privacy Act 1988 (Cth)*.

18. **Policy**: Statement of Thrive's position and actions on a specific issue.

19. **Public Domain Information**: Information accessible by the general public.

20. **Record**: Any document or in formation created, received or maintained as evident of decision, actions or transactions. Records must be authentic, reliable and usable and must be retain and disposed of in line with organisational and legal requirements.

21. **Sensitive Information**: Information that includes racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health information, or criminal record.

22. **Team Member**: All Thrive employees, volunteers and subcontractors.

23. **Thrive** means together, Thrive Care Group Pty Ltd ACN 637 232 752 and each of its subsidiaries.

References

1. Aged Care Act 2024 (Cth) and its associated regulations

2. National Disability Insurance Scheme (NDIS) Practice Standards and their associated regulations

3. Privacy Act 1988 (Cth)

4. Australian Privacy Principles (APPs)

Version Control

Version 1	31 August 2025	New policy creation

Thrive Care Group

Visit: thrivecaregroup.com.au
Email: hello@thrivecaregroup.com.au