# Information Management and Privacy

## 1. PURPOSE

Helping Hand Aged Care (Helping Hand) is committed to protecting the privacy, confidentiality, and dignity of all individuals whose information we collect, use, store, and manage.

This policy establishes a comprehensive information management and privacy governance system that safeguards personal information while supporting quality care, regulatory compliance, and transparent decision-making. It provides the foundation for managing Helping Hand's information, including consumer care records, workforce and corporate data, and stakeholder communications, in accordance with legal obligations and strategic objectives.

## 2. SCOPE

This policy applies to all aspects of information management and privacy protection within Helping Hand, establishing principles and frameworks for:

- **Individual information:** personal information and health records (residents, clients, associated providers).
- **Workforce information:** employment, health, performance and compliance records.
- **Corporate governance:** regulatory compliance, financial, risk management and accountability records.
- **Information security:** collection, sharing, retention, disposal, and privacy breach prevention.
- **Stakeholder communications:** management of external information, partnerships and reporting correspondence.

This policy ensures consistency and compliance with applicable Commonwealth and State legislation and contractual obligations, including aged care, disability, and privacy laws.

## 3. POLICY STATEMENT

This policy is a key component of Helping Hand's risk management and governance framework. It mitigates organisational risk by ensuring lawful, ethical, and secure handling of information assets, and supports Board-level oversight of privacy and data protection obligations.

Helping Hand will:

- Protect the privacy, security, and integrity of all information assets.
- Collect, use, and store personal information only for lawful and legitimate purposes.
- Ensure individuals are informed of their rights to access, correction, advocacy, and supported decision-making.
- Maintain robust information governance, cybersecurity, and business continuity systems.
- Provide training and accountability for all staff and partners handling information.
- Continuously review and improve information management practices to meet evolving legal, ethical, and operational requirements.

# 4. POLICY PRINCIPLES

Helping Hand's approach to information management and privacy is guided by the following principles:

- **Consumer-Centred**: Respecting dignity, autonomy, and privacy rights, including access, correction, advocacy, and supported decision-making.
- **Integrated**: Embedding privacy and governance across all services, systems, and organisational functions.
- **Accountable**: Ensuring leadership, and reporting structures support transparency and compliance.
- **Secure and Ethical**: Applying lawful, risk-based practices including cybersecurity, access controls, and lifecycle management.
- **Inclusive and Respectful**: Managing information in culturally and linguistically appropriate ways.
- **Collaborative**: Engaging stakeholders in co-design, feedback, and continuous improvement.
- **Resilient and Risk-Aware**: Ensuring business continuity, technology governance, and risk mitigation through robust planning, system safeguards, and incident response.
- **Continuous Improvement**: Regularly reviewing practices against legislation, best practice, and stakeholder input.
- **Governance-Driven**: Aligning with strategic risk, assurance, and quality frameworks.

# 5. POLICY REQUIREMENTS

## 5.1 Information Management System

Helping Hand's information management system encompasses all organisational information assets, including:

- Individuals' personal, health, and care information.
- Employee personal, employment, and health information.
- Corporate governance, financial, and compliance records.
- Stakeholder communications and partnership information.
- Research, quality improvement, and performance data.

**Integrated Approach:** Information management practices are integrated across all organisational functions, ensuring consistent application of privacy principles.

**Risk-Based Security:** Security measures are proportionate to the sensitivity and risk profile of different information types, with enhanced protections for highly sensitive personal and health information.

**Lifecycle Management:** Information is managed throughout its lifecycle, from collection and secure transfer through to disposal.

**Data Governance and Security Compliance:** All systems and data practices must comply with Helping Hand's Data Governance Framework and cybersecurity requirements, including data quality, access control, privacy, integrity, availability, backup/restore, and incident response.

## 5.2 Consumer Information Management

- Guided by the Statement of Rights under the Aged Care Act 2024, recognising consumers' rights to privacy, dignity, and control.
- Informed consent is obtained using accessible communication methods and supporting decision-making capacity.
- Consumers and authorised representatives have the right to access and correct personal information (Australian Privacy Principles (APPs) 12 & 13 – Access to Personal Information).

- Information sharing supports integrated, person-centred care while maintaining privacy protections.
- Privacy Collection Statements are provided at the point of collection (APP 5).
- Helping Hand complies with the My Health Records Act 2012. Staff may only access My Health Record information with consent and within authorised roles.

## 5.3 Workforce Information Management

- Employee personal information is managed in accordance with employment law and privacy principles.
- Health information, including workers' compensation and return-to-work data, is protected with enhanced confidentiality.
- Performance and development records are managed fairly and transparently.
- Worker screening and compliance records are securely retained and disposed of in line with policy.

## 5.4 Corporate Governance Information

- Managed to support Board accountability, regulatory compliance, and transparent decision-making.
- Regulatory reporting information is maintained accurately and submitted as required.
- Financial and prudential information is managed in line with governance and accounting standards.
- Risk-related information supports effective assessment, monitoring, and treatment.

## 5.5 Information Security and Protection

- Multi-layered security measures include physical security, access controls, encryption, sensitivity tagging, data loss prevention and cyber protections.
- Access to personal information is restricted to authorised personnel and reviewed regularly.
- Cybersecurity practices align with Australian Cyber Security Centre's Essential Eight mitigation strategies and the NIST Cybersecurity Framework.
- Cybersecurity oversight and incident response are coordinated through the ICT Steering Committee
- Backup and recovery procedures ensure business continuity.
- Technology governance includes safeguards for Artificial Intelligence (AI), social media, and third-party systems to ensure responsible digital transformation.
- The organisation maintains current cyber insurance and has a formal relationship with external cybersecurity experts to assist risk mitigation and cyber improvements.

## 5.6 Information Sharing and Disclosure

- Personal information is disclosed only in accordance with privacy law, including with consent, for legal obligations, or in emergencies.
- Information sharing with healthcare providers supports continuity of care while maintaining privacy protections.
- Sharing with supporters and representative's respects consumer preferences and legal authority.
- Regulatory reporting is conducted in accordance with legal and compliance obligations.

## 5.7 Privacy Breach and Incident Management

- Proactive measures are in place to prevent privacy breaches through training, system design, and risk assessment.
- Breaches are responded to rapidly with containment, investigation, and remediation.
- Serious or repeated breaches are escalated to the Aged Care Quality and Safety Commission.

- Affected individuals and regulators are notified in accordance with legal requirements.
- Incidents inform continuous improvement of privacy and security practices.
- Privacy breach management aligns with Helping Hand's Feedback, Complaints & Whistleblower Management Policy.
- Consumers and staff may raise concerns without fear of reprisal.
- All incidents are reviewed to strengthen practices and inform training and system updates.

## 6. ROLES & RESPONSIBILITIES

### Helping Hand Board

- Provide strategic oversight and governance of information management and privacy.
- Approve and review the policy and major updates.
- Ensure alignment with Helping Hand's strategic vision, legal obligations, and the Statement of Rights.
- Monitor privacy and information governance performance through Board reporting.
- Promote a culture of accountability and transparency.
- Allocate resources for compliance, risk mitigation, and continuous improvement.
- Oversee risk and assurance functions, including audits and privacy breach trends.

### Executive Management Team

- Lead implementation of the policy and ensure operational alignment with strategic objectives.
- Develop and maintain supporting procedures and frameworks.
- Monitor compliance and report to the Board.
- Oversee privacy breach response and legal notification processes.
- Allocate resources for training, systems, and secure infrastructure.
- Align governance with Helping Hand's risk appetite and business continuity planning.

### Managers and Supervisors

- Operationalise the policy within teams and service areas.
- Communicate policy expectations and provide role-specific training.
- Monitor team compliance and escalate issues.
- Support continuous improvement and risk mitigation.
- Manage privacy during recruitment, performance, and workforce planning.
- Respond to and escalate privacy incidents.

### Privacy Officer

- Provide expert oversight of privacy compliance and breach management.
- Ensure compliance with privacy laws and aged care standards.
- Deliver training and guidance to staff.
- Lead investigations into privacy breaches and coordinate remediation.
- Liaise with regulators (OAIC, ACQSC).
- Advise on privacy frameworks, contracts, and regulatory obligations.

### All Employees

- Comply with privacy and information management requirements in daily work.
- Protect confidentiality and report breaches or concerns.
- Participate in training and follow procedures.
- Support consumer rights and advocacy access.

- Maintain confidentiality during and after employment.
- Contribute to feedback and improvement initiatives.

### Residents and Clients

- Exercise their rights to privacy, access, and control over personal information.
- Provide informed consent for collection and use of personal information.
- Request access to or correction of their records.
- Raise concerns or complaints about privacy or information handling.
- Engage in co-design and feedback processes.
- Nominate supporters, representatives or advocates as needed.

### Supporters, Advocates, and Representatives

- Support residents and clients in exercising their privacy rights and making informed decisions.
- Act in accordance with the consumer's wishes and legal authority.
- Assist with understanding privacy information and consent.
- Communicate with Helping Hand on behalf of the consumer where authorised.
- Support access to advocacy services (e.g., ARAS, OPAN).
- Respect confidentiality and privacy obligations.

### External Service Providers (e.g., IT vendors, associated providers)

- Handle Helping Hand information in accordance with contractual, legal, and ethical obligations.
- Comply with Helping Hand's privacy and information security requirements.
- Ensure secure handling, storage, and disposal of Helping Hand data.
- Report data breaches or security incidents immediately.
- Participate in privacy training or onboarding where required.
- Cooperate with audits or investigations related to information management.
- All individuals and committees share collective responsibility for ensuring Helping Hand's information management practices uphold integrity, transparency, and respect for individual rights.

## 7. MONITORING AND COMPLIANCE

The Board exercises due diligence over information management through the following mechanisms:

- **Internal Audits**: Regular audits of information management and security practices.
- **Cybersecurity Risk Assessments**: Periodic assessments to identify vulnerabilities and ensure appropriate technical and organisational controls are in place.
- **Incident and Training Reviews**: Review of information security incidents, breaches, and training compliance records.
- **Legislative Compliance:** Systems are in place to ensure compliance against the requirements of the Privacy Act 1988, Aged Care Act 2024, and My Health Records Act 2012
- **Audit and Assurance Activity:** Independent audits and assurance reviews to verify the integrity, confidentiality, and availability of information systems.
- **Risk Reporting:** Regular review of enterprise risks relating to information management, cybersecurity, and privacy as part of the integrated Enterprise Risk Management Framework
- **Governance Oversight:** Oversight and reporting through the ICT Committee, Executive Risk Management Committee, and the Board.
- **Actioning Findings:** Audit and incident findings are tracked through the Continuous Improvement Register and Risk Management Framework, with assigned actions monitored and reported to the Board.

## 8. MANDATORY RELATED DOCUMENTS

The following documents must be complied with under the Policy, to the extent that they are relevant:

**Internal Documents**

- Privacy Policy
- Records Management Policy
- Data Security & Cyber Risk Management Policy
- Digital Technology Governance Policy (including AI, social media use, and communications)
- Information Sharing and Disclosure/Provision Policy
- Clinical Governance Framework (QAL021P)
- Risk Management Framework (QAL022P)
- Quality and Safety Management System
- Information Systems Data Governance Framework (ISD017P)
- Cyber Security Response Plan (ISD018P)
- Backup Procedure
- Information Systems Continuity Plan (ISD016P)
- Document Governance Framework (QAL038P)
- Organisational Archiving Procedure (CSS001P) and Record Retention Schedule
- Consumer Engagement Strategy
- Workforce Development Framework
- Privacy Procedures

**External References**

- New Aged Care Act 2024
- New Aged Care Rules 2025
- Strengthened Aged Care Quality Standards
- National Disability Insurance Scheme Act 2013
- NDIS Practice Standards and Quality Indicators
- Aged Care Statement of Rights
- Privacy Act 1988 (Commonwealth) and Australian Privacy Principles
- My Health Records Act 2012 (Commonwealth)
- Cyber Security Act 2024
- Fair Work Act 2009 (Commonwealth)

## 9. SUPPORTING INFORMATION

- Australian Cyber Security Centre (ACSC) Essential Eight

## 10. DEFINITIONS AND ABBREVIATIONS

| Word/Term | Definition |
|---|---|
| **Access Request** | A request by an individual to view or obtain a copy of their personal information held by Helping Hand. |
| **Board** | means the Helping Hand Aged Care Inc. Board of Directors. |
| **Breach** | An incident where personal or sensitive information is lost, accessed, disclosed, or used without authorisation. |

| Word/Term | Definition |
|---|---|
| **Confidentiality** | The obligation to protect information from unauthorised access or disclosure. |
| **Consumer** | Any person receiving aged care or wellbeing services from Helping Hand |
| **Data Breach Notification** | The process of informing affected individuals and regulators of a notifiable data breach under law. |
| **Data Governance** | The framework for managing data availability, usability, integrity, and security. |
| **Employees (Workforce)** | means all Helping Hand employees, contractors, volunteers, students and others acting on behalf of Helping Hand etc. |
| **Governance** | The processes and structures used to direct and manage Helping Hand. |
| **Helping Hand** | Helping Hand Aged Care Inc. (ABN: 19 636 743 675) |
| **Information Asset** | Any data, record, or document that has value to Helping Hand's operations or compliance. |
| **Information Management** | The policies, processes, and systems for collecting, storing, using, sharing, and disposing of information. |
| **Personal Information** | Information or an opinion about an identified individual, or an individual who is reasonably identifiable. |
| **Privacy** | The right of individuals to control the collection, use, and disclosure of their personal information. |
| **Privacy Breach** | Any unauthorised access, disclosure, or loss of personal information. |
| **Sensitive Information** | A subset of personal information that includes health, racial or ethnic origin, political opinions, religious beliefs, or criminal record. |
| **Serious or Repeated Breach** | A *serious breach* involves unauthorised access or loss of information likely to cause significant harm. A *repeated breach* indicates recurring issues or systemic failure. These must be escalated to the Executive and reported to regulators as required. |
| **Statement of Rights** | The statutory list of rights for people receiving Australian Government-funded aged care services |
| **Cyber Security** | The protection of information systems from theft, damage, or unauthorised access. |

## 11. GOVERNANCE

This policy is approved by the Board and reviewed annually, or sooner if required, to ensure alignment with Helping Hand's strategic objectives, governance frameworks, and legislative obligations.

| **Version** | **1.0** |
|---|---|
| **Endorsement/ Approval Date** | 28 October 2025 |
| **Approved By** | Board |
| **Review Cycle** | Every 3 years, or as required. |
| **Due for Review** | 28 October 2028 |
| **Document Owner** | Board |

### Review Cycle and Approval Process

This policy will be reviewed every three years by the Board in consultation with relevant stakeholders. All changes require approval by the Board

### Communication of the Policy

This policy will be communicated via:

- Staff training and onboarding.
- Intranet updates and email notifications.

### Summary of Changes

| Version | Date | Changes |
|---|---|---|
| 1.0 | 28 October 2025 | Initial document. |