CONFIDENTIALITY AND PRIVACY POLICY AND PROCEDURE

Date created	November 2007
Version number	V12, June 2026
Policy administrator	Head of Strategic Relations and Quality
Review date	June 2028
Located	Library
If you have queries regarding this document, or proposed changes, please contact the Quality and Compliance Lead	

Contents

1. OUR COMMITMENT

Lutheran Care (LC) is committed to safeguarding the privacy and confidentiality of all people who access its services, work for, or engage with the organisation.

This policy is informed by, and complies with, applicable Commonwealth, State and Territory privacy, information sharing, child protection, disability and records management legislation, including the *Privacy* Act 1988 (Cth) and subsequent reforms.

This policy has been updated to reflect significant legislative amendments introduced under the *Privacy and Other Legislation Amendment* Act 2024 (Cth), which strengthen individual privacy rights, data security obligations, enforcement powers and remedies.

Privacy laws establish national and state-based standards for the collection, use, disclosure, storage and disposal of personal information and aim to ensure that information is handled in a lawful, fair, transparent and secure manner.

This policy forms part of LC's broader governance, risk and compliance framework and supports organisational accountability for privacy, confidentiality and information management.

NOTE: Refer to the *Employee Records Policy* for the policy and procedure to be followed regarding employee records.

For staff who are authorised family law counsellors (refer to the *Authorised LC staff for Family Law Counselling Purposes* document in the Library) - before any client information is released / used outside of the client / practitioner agreed upon parameters (mandatory reporting not included), additional considerations may be required as to ensure compliance with *Family Law* Act 1975 and the *Family Law Amendment* Act 2023. Please seek Manager advice **before sharing any client information**.

2. PURPOSE

The purpose of this policy is to:

- outline LC's legal and ethical obligations in relation to privacy and confidentiality
- describe how personal and sensitive information is collected, used, stored, disclosed and disposed of
- ensure people understand their rights in relation to their personal information, including access, correction and complaints, and
- support compliance with privacy, child safety, disability and information sharing legislation.

This policy also reflects LC's obligation to take proactive and reasonable steps to prevent privacy breaches, including the implementation of technical and organisational security measures.

3. SCOPE

3.1 This policy applies to all workers, volunteers, students, contractors, consultants and Board Members, who will be collectively referred to as 'workers' for the purpose of this document.

3.2 This policy covers personal information collection regarding:

- workers, contractors, volunteers, students, consultants, applicants for employment and board members, and
- donors and prospective donor information.

3.3 Where a funding agreement has specific requirements pertaining to the collection and storage of sensitive information that are outside this policy, a separate procedure may exist, or will be developed as necessary, and will be an extension of this policy as to ensure compliance with the overarching program contract.

4. POLICY

4.1 LC respects the dignity, privacy and confidentiality of all people and is committed to handling personal information in accordance with applicable legislation and best practice.

4.2 LC will:

- only collect information that is necessary for service provision or organisational functions
- use and disclose information only for lawful, authorised and transparent purposes
- store information securely and restrict access to authorised personnel
- retain and dispose of information in accordance with legislative and evidentiary requirements, and
- respond promptly and appropriately to privacy complaints and breaches.

4.3 LC recognises that individuals have the right to take action where personal information is misused, including seeking remedies under applicable privacy laws.

4.4 Confidentiality is not absolute. Information may be shared without consent where required or authorised by law, or where there is a risk to safety or wellbeing.

5. PRINCIPLES GOVERNING PRIVACY AND CONFIDENTIALITY

LC adheres to the following principles:

- **Lawfulness and fairness** – information is handled in accordance with law and ethical standards.
- **Transparency** – people are informed about what information is collected and how it will be used.
- **Purpose limitation** – information is only used for the purpose for which it was collected.
- **Data minimisation** – only necessary information is collected and retained.
- **Accuracy** – reasonable steps are taken to keep information up to date.
- **Security** – information is protected against misuse, interference, loss, unauthorised access or disclosure.
- **Accountability** – LC accepts responsibility for its privacy practices and compliance.
- **Storage limitation** - information is retained only for as long as necessary and disposed of in line with legal and organisational requirements.

- **Individual rights** – individuals can access, correct and seek information about how their personal data is handled.
- **Risk management and breach response** – risks to personal information are actively managed, and breaches are identified, reported and responded to promptly (refer to the *ICT Data Breach Response Policy and Procedure*).

6. COLLECTION OF PERSONAL INFORMATION

LC collects personal and sensitive information only where it is:

- necessary to provide services
- required or authorised by law or contract
- reasonably required for organisational functions

Information is collected directly from individuals where possible. In some circumstances, information may be collected from third parties where it is unreasonable or impracticable to collect it directly, or where permitted by law.

Clients will be informed, at or before the time of collection, of:

- the purpose of collection
- how their information will be used and disclosed
- the consequences of not providing information
- their right to access and correct their information
- how to make a complaint

Where services are provided to children or vulnerable persons, additional care is taken to ensure consent is informed, lawful and appropriate to the individual's capacity.

Where unsolicited personal information is received, LC will determine whether it could have been collected in accordance with this policy. If not, the information will be securely destroyed or de-identified where lawful and practicable.

7. USE AND DISCLOSURE OF PERSONAL INFORMATION

LC will only use or disclose personal information:

- for the primary purpose for which it was collected
- for a related purpose that would be reasonably expected
- with consent, and
- where required or authorised by law

LC may disclose information to:

- partner organisations and service providers
- government agencies and regulators, and
- other parties where required for service delivery or safety

Only the minimum necessary information will be used or disclosed.

8. INFORMATION SHARING GUIDELINES (ISG)

LC applies the *South Australian and Northern Territory Information Sharing Guidelines (ISG)* when working with children, young people and adults experiencing vulnerability and risk.

Information sharing decisions must:

- prioritise the safety and wellbeing of individuals
- consider and seek consent wherever safe and practicable

- recognise that information may be shared without consent where permitted or required by law, including where there is a risk to safety or wellbeing
- ensure that only the minimum necessary information is shared
- be made in accordance with legislative requirements and internal delegations, and
- be clearly documented, including the rationale for the decision, whether consent was sought or obtained, and any risk considerations

The application of the ISG **does not override mandatory reporting obligations**, and workers must comply with all legal requirements to report concerns relating to child protection, safety, or reportable incidents.

9. MANDATORY REPORTING

All workers must comply with applicable child protection legislation and organisational requirements in relation to safeguarding and reporting concerns.

Relevant legislation includes:

- *Children and Young People (Safety)* Act 2017 (SA)
- *Care and Protection of Children* Act 2007 (NT)

Certain roles are designated as mandated reporters and are legally required to make a report as soon as practicable where there are reasonable grounds to suspect that a child or young person is at risk of harm.

Where individuals are mandated reporters, this obligation applies personally and cannot be delegated.

All workers (regardless of mandated status) are required to:

- take all concerns regarding child safety seriously
- escalate concerns in line with organisational procedures, and
- support the reporting process where required

A report must be made:

- based on reasonable suspicion, and
- without delay, and must not be postponed to seek internal approval

While workers are encouraged to seek guidance and support from their manager or supervisor, **this must not delay or prevent** a report being made. For further information refer to the *Child Safe Policy and Procedure.*

Mandatory reporting obligations override confidentiality and consent requirements, and information must be disclosed where required to protect a child or young person.

LC will support workers to meet their reporting obligations and ensure appropriate documentation and follow-up actions are completed.

10. NDIS QUALITY AND SAFEGUARDS COMMISSION

As a registered NDIS provider, LC is required to report reportable incidents to the NDIS Quality and Safeguards Commission in accordance with legislative requirements.

All workers must:

- take immediate action to ensure the safety and wellbeing of the participant, and
- report all incidents, allegations, and concerns immediately through LC's internal incident reporting processes (refer to the *Client Incident Management Policy and Procedure).*

LC will ensure that reportable incidents are notified to the NDIS Commission within required timeframes.

Reportable incidents include alleged or suspected:

- death of a person with disability

- serious injury or psychological harm
- abuse or neglect
- unlawful sexual or physical contact
- sexual misconduct

These incidents **must be reported to the NDIS Commission within 24 hours** of becoming aware of a reportable incident. For further information please refer to the *Elcies Incident Management Policy and Procedure*, and the *Elcies Reportable Incidents Involving the Use of a Restricted Practice Policy and Procedure.*

Unauthorised use of restrictive practices must be reported within 5 business days.

LC will:

- submit all required follow-up information within statutory timeframes
- maintain appropriate records and documentation, and
- ensure incidents are reviewed and managed in line with organisational policies and regulatory requirements

11. DATA SECURITY AND DIGITAL INFORMATION

LC will take reasonable steps, including technical and organisational measures, to protect personal information held electronically and in hard copy from misuse, interference, loss, and unauthorised access or disclosure.

This includes:

- access controls and user authentication, ensuring information is accessed on a need-to-know basis
- secure storage systems for both digital and physical records
- encryption and secure transmission of information where appropriate
- appropriate management of devices, including mobile and remote access
- workers training and awareness of information security responsibilities
- monitoring and auditing of data access and system use

LC will also take steps to:

- identify, report and respond to actual or suspected data breaches in accordance with organisational procedures
- ensure that third-party service providers and systems handling personal information meet appropriate security standards
- securely store and dispose of physical records, including the use of locked storage and confidential waste processes

This reflects strengthened data security obligations under the *Privacy* Act 1988 (Cth). For more information regarding LC internal policies and procedures about data security and digital information, please refer to the *Information Communication and Technology* area of the Library.

12. AUTOMATED DECISION-MAKING

LC does not use automated or technology-assisted systems that significantly impact individuals with processes such as eligibility, service access or support decisions.

LC will ensure transparency in accordance with legislative requirements, and individuals will be informed if automated decision-making is used and how this may affect them.

13. RECORDS MANAGEMENT AND RETENTION

Records will be retained:

- for as long as required by law
- where necessary for service continuity, accountability, or risk management, and
- in accordance with applicable legislation, including the *State Records* Act 1997 (SA), *Information* Act 2002 (NT), and the National Disability Insurance Scheme Act 2013 (Cth).

Records must only be destroyed in accordance with approved retention and disposal schedules and organisational procedures.

Records relating to children, abuse, neglect, serious incidents or Aboriginal and Torres Strait Islander clients will not be destroyed unless legally permitted.

Records must not be destroyed where they are:

- subject to a complaint, investigation or legal proceedings, or
- required for audit, review or regulatory purposes

General retention guidelines include:

- financial records – minimum of 7 years
- NDIS records – retained in line with evidentiary and regulatory requirements, and
- child protection records – retained indefinitely where required

LC will ensure that:

- records are maintained in a manner that preserves their integrity, accuracy and accessibility
- records are securely stored and protected from unauthorised access, and
- records are securely destroyed or de-identified when no longer required, including through approved physical and digital disposal processes

14. BREACHES OF CONFIDENTIALITY AND DATA BREACHES

Any suspected or actual breach of privacy or confidentiality must be reported immediately through LC's internal reporting processes, with the Executive Manager responsible for Quality and Service Delivery as well as, the Chief Executive officer (CEO) being informed in accordance with internal escalation requirements. Refer to *Client Incident Management Policy and Procedure,* and the *ICT Data Breach Response Policy and Procedure* for further information.

LC will:

- promptly assess and investigate all suspected or actual breaches
- take immediate steps to contain the breach and minimise harm
- determine whether the breach constitutes an eligible data breach under the Notifiable Data Breaches Scheme
- notify affected individuals, relevant contract manager / funder, and the Office of the Australian Information Commissioner where required, and
- implement corrective actions to prevent recurrence.

Assessments of suspected data breaches will be undertaken as soon as practicable and within required timeframes.

LC complies with the Notifiable Data Breaches Scheme under the *Privacy* Act 1988 (Cth) and recognises the expanded enforcement powers of the Office of the Australian Information Commissioner. Refer to *ICT Data Breach Response Policy and Procedure.*

Serious breaches may expose LC to regulatory penalties and civil liability.

15. ACCESS TO PERSONAL INFORMATION

Individuals have the right to:

- request access to their personal information, and
- request correction of inaccurate, incomplete or out-of-date information

Requests for access or correction must be made in accordance with LC's processes and will require verification of identity prior to information being released (refer to *Request for Access to Personal Records* form).

Requests will be responded to within a reasonable period, in line with legislative requirements (refer to *Process Map for handling client requests to access personal records*).

Access may be refused or limited where permitted by law, including where:

- providing access would pose a serious threat to the life, health or safety of any person
- the information relates to another individual and cannot be reasonably separated, and
- access would prejudice legal proceedings or investigations

Where access is refused or limited, individuals will be provided with an explanation in accordance with legal requirements.

Where a request for correction is made, LC will:

- take reasonable steps to correct the information where it is satisfied it is inaccurate, incomplete or out-of-date, and
- where appropriate, associate a statement with the information if a correction is not made

Access will be provided in a manner that is reasonable and practicable, having regard to privacy, safety and operational, and contractual considerations.

16. RESPONSIBILITIES

All workers are responsible for:

- understanding and complying with this policy
- handling personal and sensitive information appropriately and in line with legislative and organisational requirements
- maintaining confidentiality
- promptly reporting any concerns, risks or actual breaches of privacy or confidentiality, and
- complete privacy and confidentiality training as required.

Managers are responsible for:

- ensuring workers are aware of, understand, and comply with this policy
- providing appropriate guidance, education and support to enable workers to meet their obligations
- reinforcing expectations for information handling and confidentiality in day-to-day practice
- monitoring compliance within their teams and addressing any issues or risks, and
- ensuring concerns, incidents or breaches are appropriately escalated and managed in line with organisational processes

Executive are responsible for:

- providing organisational leadership and oversight of privacy, confidentiality, and information management
- ensuring appropriate governance frameworks, systems and controls are in place
- monitoring organisational compliance, risk and performance in relation to privacy obligations
- ensuring adequate resources, training and capability are available to support compliance, and

- responding to significant risks, incidents or breaches and ensuring appropriate organisational action

17. REVIEW AND GOVERNANCE

This policy is owned by the Executive Manager responsible for Quality and Service Delivery and is approved by the Chief Executive Officer (or delegate).

This policy will be reviewed at least every two years, or earlier where:

- legislative or regulatory changes occur
- there are significant changes to organisational operations or systems, or when
- incidents, audits or reviews identify a need for update

Compliance with this policy will be:

- monitored through organisational processes, including audits, reviews and incident management, and
- reported through appropriate governance and risk frameworks

18. PRIVACY COMPLAINTS

Individuals may make a complaint about the handling of their personal information. Refer to the *Feedback and Complaint Handling Policy and Procedure.*

Complaints can be made to:

- LC via our website, https://lutherancare.tod.net.au/incidents/new/ed29aa11b5358e8da86e9515573f96a1
- Via email feedback@lutherancare.org.au
- Via LC QR code

- Or in writing to

  Lutheran Care
  PO Box 1020
  Prospect East SA 5082

LC will:

- acknowledge complaints promptly
- investigate and respond within a reasonable timeframe, and
- take appropriate action to resolve issues

If an individual is not satisfied with the response from LC, they may escalate their complaint to the program funder (contract manager details / process details can be provided by the program manager), and / or the Office of the Australian Information Commissioner (OAIC is an independent Australian government statutory agency, established under the *Australian Information Commissioner* Act 2010 (Cth), responsible for regulating

privacy and freedom of information (FOI). It protects individuals' privacy rights, handles information access disputes, and ensures the proper handling of personal information).

PROCEDURE

19. PURPOSE

This procedure outlines how workers apply confidentiality and privacy requirements in practice, thereby supporting the standards outlined in the policy section.

20. SCOPE

This procedure applies to all workers who handle personal or sensitive information in the course of their work with LC.

21. HANDLING CONFIDENTIAL INFORMATION IN PRACTICE

21.1 Accessing information

Workers must only access information that is directly required to perform their role and must not access records out of curiosity or for personal interest.

All information must be accessed, viewed, and stored using approved organisational systems and locations.

Workers must also ensure systems are logged out of and information is secured when not in use.

21.2 Discussing client information

When discussing client information, workers must:

- ensure conversations occur in private settings (e.g. offices or meeting rooms) and not in open or shared areas where they may be overheard by members of the public,
- only share information with authorised workers involved in the client's care or service delivery, and
- share only the minimum necessary information relevant to the discussion.

21.3 Maintaining confidentiality

Workers must:

- ensure emails, messages and documents containing personal information are sent only to the correct recipients,
- ensure all documents are securely stored, and
- client information must not be left visible on screens or desks where it can be accessed or viewed by unauthorised persons.

Workers must not:

- disclose, confirm or deny whether a person is a client of LC unless authorised, or
- share client information with family external parties unless appropriate consent or legal authority exists.

21.4 Responding to requests for information

If any person requests information about a client, workers must:

1. Do not disclose any information, including:
    - confirming whether the person is a client,
    - providing contact details or location, or

- share any personal or service information.

2. Advise the person politely that you are unable to provide information due to confidentiality requirements.

3. Refer the request appropriately:
   - to the client directly, where appropriate, or
   - to a manager or formal process if required.

4. Where appropriate, and if safe to do so:
   - inform the client that someone has attempted to contact them / seek information about them, and
   - allow the client to decide whether they wish to respond.

If workers are unsure whether information can be shared, they must:

- not disclose the information,
- seek guidance from their manager or supervisor, and
- follow the Information Sharing Guidelines (ISG) where relevant.

21.5 Responding to client requests for access to information

When a client requests access to information the organisation holds about them, workers must ensure the request is managed in accordance with confidentiality and privacy requirements.

Refer to *Process Map for handling client requests to access personal records* for further information.

21.5.1 Receive and record the request

Requests must be made in writing using the *Request to Access Personal Records form* and must be acknowledged promptly. Workers must clarify the scope of the request where required and document the request in the client record, including the date, details of the information requested, and how / why the request was made. The request must be escalated to the relevant manager for processing.

If further information / guidance is required, contact can be made with the Quality and Compliance Lead.

21.5.2 Verify identity and assess the request

Workers must confirm the identity of the client before releasing any information. Requests from third parties must not proceed without documented client consent or appropriate legal authority. The request must be assessed in consultation with a manager and / or Quality and Compliance, taking into account privacy obligations, legislation, and any risks associated with disclosure, including third-party information.

21.5.3 Prepare and provide access

Information must be reviewed prior to release to ensure it is appropriate, accurate, and lawful to share. Workers must redact any third-party or restricted information and determine the most appropriate method of access (e.g. copies, supervised review, or summary). Information must be provided in a timely and secure manner, and workers should offer to explain the information or support the client to understand it where appropriate.

21.5.4 Communicate outcomes and document

Workers must clearly communicate the outcome of the request. Where access is approved, confirm what has been provided. Where access is limited or declined, provide a clear explanation and outline available options, including review or complaints processes. All actions, decisions, and information released must be documented in the client record.

21.5.5 Escalation and guidance

If workers are unsure at any stage, they must not release information and must seek guidance from their manager or Quality and Compliance. Complex or high-risk matters must be escalated immediately.

22. RECORDING INFORMATION

Workers must ensure that any information recorded about clients is:

- relevant, necessary, and appropriate for service delivery,
- accurate and recorded in a timely manner, and
- managed and stored securely within approved systems.

All documentation must be completed in accordance with organisational policies, including the *Case Noting Practice Guide* and associated training.

23. USE OF RECORDINGS, PHOTOGRAPHS AND MEDIA

23.1 Audio and Video Recording

Workers must comply with applicable legislation, including the:

- *Surveillance Devices* Act 2016 (SA)
- *Surveillance Devices* Act 2007 (NT)

Audio or video recording of any individual must not occur without prior informed consent. Refer to the *Workplace Surveillance Policy* for more information.

Workers must ensure that:

- informed consent is obtained before recording any interaction,
- consent is voluntary, informed and documented where required,
- individuals understand the purpose and intended use of the recording,
- recordings are only used for the agreed and authorised purpose, and
- recordings are stored securely and accessed only by authorised personnel.

Unauthorised recording of clients, workers or volunteers is strictly prohibited.

23.2 Photographs and Video

Photographs or video footage must not be taken or used without prior informed consent. Refer to the *Photographs and Video Footage Policy and Procedure* for more information.

Workers must ensure that:

- written consent is obtained before capturing or using images,
- the purpose and intended use is clearly explained,
- images are only used for the specific purpose consented to, including any promotional use, and
- images and footage are stored securely and accessed only by authorised personnel.

Additional care must be taken when working with children, young people, Aboriginal, and Torres Strait Islander people and vulnerable persons, including:

- obtaining consent from a parent, guardian or authorised representative where required,
- ensuring the safety, dignity and best interests of the individual, and
- avoiding identification where this may create risk.

Images or footage must not be shared:

- on social media or external platforms without explicit consent (refer to the *Social Media Policy and Procedure* for more information), or
- in a way that identifies a person's location, identity or personal circumstances where this may create risk.

24. INFORMATION SHARING IN PRACTICE

Workers must follow the steps below when considering whether to share client information.

24.1 Consider whether information can be shared and what type of information

All information sharing must be:

- guided by the Information Sharing Guidelines (ISG),
- based on client consent, wherever safe and practicable, or

Information may be shared without consent where:

- it is permitted or required by law, and / or
- there is a risk to the safety or wellbeing of the client or others.

Apply the Minimum Necessary Principle. Only share information that is:

- directly relevant to the purpose,
- limited to what is necessary, and
- do not disclose excessive or unrelated information.

Use the *ISG Decision Making Steps and Practice Guide* to guide your decision. Consider:

- purpose of sharing
- level of risk
- consent status, and
- cultural considerations (refer Section 7 of the *Information Sharing Procedure*)

Seek approval where required

- Do not share information without consent unless approval has been obtained from the appropriate delegate.
- Approval is required for:
  - sharing information without client consent
  - decisions to refuse to share information, where applicable
- Refer to the approval levels in the table found at the end of this section .
- If you are unsure whether information can be shared, you must not disclose the information and must seek guidance from your line manager or supervisor before taking any action.

Share information securely

- When sharing information:
  - use approved and secure communication methods, and
  - ensure the recipient is authorised to receive the information

Document the Decision

- Record in the client file:
  - what information was shared (or not shared)
  - who it was shared with
  - whether consent was obtained or not
  - the rationale for the decision, and
  - any approvals obtained

Workers must:

- share only the minimum necessary information,
- document decisions and rationale for sharing, and
- escalate concerns when unsure.

The *ISG Decision Making Steps and Practice Guide* clearly sets out the steps to be followed. The decision to share **without consent must be approved** by a manager or supervisor (see table below) and be documented according to the lines of approval in the ISG.

Positions providing service to clients / community	**Is approval required from line manager for information sharing:** • Without consent • When refusing to share?	**Line manager, supervisor, coordinator**
Team Leaders, Managers, Supervisors, Volunteer Coordinators	Yes	Executive Manager, Operations Manager, Program Manager
Case Workers	Yes	Team Leaders, Supervisors
Program Support Team Members	Yes	Team Leaders
Finance, Administration*	Yes	Executive Manager
HR Workers*	Yes	Executive Manager

Additional Guidance

- Workers must also consider cultural safety and appropriateness when sharing information.
- Refer to Section 7: *Cultural Considerations in the Information Sharing Procedure*.

25. DISCLOSURE OF INFORMATION

Personal information may only be disclosed with client consent, for legitimate service delivery purposes, or where required or authorised by law. Workers must ensure consent is documented where required, must not disclose information to third parties without appropriate authority, and must refer all external requests for information (including subpoenas or requests from agencies) to their manager.

26. DATA SECURITY

Workers must take all reasonable steps to protect client and organisational information from unauthorised access, loss, or misuse.

All workers are responsible for maintaining the security, integrity, and confidentiality of information at all times, including when working remotely or offsite.

Workers must ensure that all devices are password protected, locked when unattended, and not left in unsecured or visible locations. Systems must be accessed using individual logins only, and passwords must not be shared. Workers must log out or lock systems when not in use.

Confidential information must only be stored in approved organisational systems. Workers must not store information on personal devices, USBs, or unauthorised platforms, or use personal email or messaging services for client information.

Hard copy information must be stored securely, not left visible in shared spaces, and collected promptly from printers or common areas. Confidential materials must be disposed of using approved secure methods, such as confidential bins or shredding, and not placed in general waste.

Any risks or breaches, including lost or stolen devices or inappropriate access or disclosure of information, must be reported immediately to a manager and managed in accordance with organisational incident and data breach procedures.

27. SOCIAL MEDIA AND COMMUNICATION

Workers must maintain professional boundaries and protect client confidentiality when using social media and communication platforms.

Client confidentiality and professional boundaries must be maintained at all times, including outside of work hours and on personal accounts.

Workers must not:

- share or discuss client information on social media or online platforms
- identify clients, or disclose their location or personal details, or
- accept or initiate personal social media connections with clients where a professional relationship exists

All use of social media and digital communication must comply with organisational policies (refer to *Social Media Policy and Procedure*).

If unsure, workers must not engage and seek guidance from their manager.

28. DEBRIEFING AND PROFESSIONAL DISCUSSION

Client information may be shared internally for legitimate professional purposes, including service delivery, supervision, risk management, and organisational oversight. Such discussions must balance client confidentiality with the organisation's responsibility for safety, quality, and risk management.

Workers may discuss client matters within supervision, team meetings, or other approved organisational forums for purposes such as service coordination, risk assessment, professional support, and incident, complaint, or practice review.

Client information must be made available to Executive and authorised senior leaders where required for incident management, risk escalation, complaints handling, and quality and safety oversight. This access must be limited to what is necessary and managed in accordance with confidentiality and privacy requirements.

Workers must ensure all discussions remain confidential, occur in appropriate settings, and involve only authorised personnel. Only relevant and necessary information may be shared.

Where appropriate, clients should be informed that their information may be discussed within the organisation to support safe, effective, and quality service delivery.

29. INCIDENTS AND BREACHES

All suspected or actual breaches of confidentiality or privacy must be treated seriously and responded to immediately.

Prompt reporting and escalation are critical to minimising harm, meeting legal obligations and ensuring appropriate organisational response

Identify and Act Immediately

A breach may include unauthorised access, use or disclosure of information, lost or stolen devices or documents, or information sent to the wrong person. If a breach is suspected or confirmed, workers must

immediately stop the activity and take reasonable steps to contain the breach and prevent further disclosure. Refer to *ICT Data Breach Response Policy and Procedure* for more information).

Report and Escalate

Workers must notify their line manager or supervisor immediately and report the incident through the Ticket incident reporting system as soon as possible (refer to the *Client Incident Management Policy and Procedure)*.

Do Not Manage Independently

Workers must not attempt to investigate, resolve, or communicate about the breach independently, and must not contact external parties (including clients) unless directed.

Preserve and Support

Workers must not alter or delete records related to the breach and must retain all relevant information to support investigation. Workers are required to cooperate with management and provide accurate and timely information as requested.

Communication and Documentation

All communication with clients, external agencies, or regulators must be undertaken only by authorised personnel. The incident must be fully documented in the reporting system and updated as required throughout the investigation.

All breaches will be managed in accordance with the *Confidentiality and Privacy Policy* and organisational incident management and data breach procedures.

30. RECORDS MANAGEMENT IN PRACTICE

Workers must ensure all client and organisational information is recorded, stored, and managed securely and in accordance with organisational requirements and;

- record information in the approved system in a timely manner
- ensure records are accurate, relevant, and complete
- store all information in approved organisational systems only
- transfer any temporary notes into the system and securely dispose of them, and
- ensure records are kept secure and only accessed by authorised personnel.

Workers must not store information on personal devices, USBs, or unauthorised platforms, use personal email or messaging services for client information, retain information outside approved systems, or delete or dispose of records independently.

Records must be managed in accordance with relevant legislative and contractual requirements. If you are unsure, you must seek guidance from your manager or supervisor before taking any action.

31. CULTURAL CONSIDERATIONS (ABORIGINAL AND TORRES STRAIT ISLANDER PEOPLES)

LC celebrates Aboriginal and Torres Strait Islander cultures as the oldest continuing cultures in the world. We recognise Aboriginal and Torres Strait Islander Peoples as the traditional custodians of the land and respect their deep spiritual connection to land and water. We acknowledge the trauma, grief and loss of both past and present.

LC recognises the importance of culturally safe and respectful handling of information relating to Aboriginal and Torres Strait Islander peoples.

Workers must ensure that:

- information is handled in a way that is culturally respectful and appropriate

- additional care is taken when collecting, recording or sharing information that may be culturally sensitive
- consent processes consider the role of family, kinship networks and community, where appropriate, and
- cultural knowledge and information is not treated as standard personal information and is managed with appropriate sensitivity.

When using images, recordings or personal information, workers must:

- be aware of cultural sensitivities relating to the use of names and images of deceased persons
- take steps to ensure that use or disclosure does not cause cultural harm, and
- seek guidance where unsure about culturally appropriate practice.

Records relating to Aboriginal and Torres Strait Islander individuals, families or communities must be handled with particular care and must not be destroyed except where legally permitted.

Where there is uncertainty about culturally appropriate handling of information, workers are encouraged to seek guidance from:

- Aboriginal workers or cultural advisors, or
- supervisors or managers.

Regarding Aboriginal and Torres Strait Islander clients, workers and volunteers, and as per section 5.19, LC will not dispose of any records relating to Indigenous individuals, families or communities or to any children. This recommendation is one of the 54 recommendations made within the '*Bringing them Home: the Report of the National Inquiry into the Separation of Aboriginal and Torres Strait Islander Children form their Families'* to support healing and reconciliation for the Stolen Generations and their families.

32. RESPONSIBILITIES

It is the responsibility of the Chief Executive Officer, the Executive Management team, all Site Managers and Service Delivery Leaders to ensure this policy is implemented. In the event further information regarding record management is required please contact the Head of Strategic Relations and Quality.

33. DEFINITIONS

Term	Meaning
Confidentiality	Confidentiality refers to the obligation of organisations that collect information to ensure that no persons or organisation is likely to be identified from any data released (*taken from the Australian Bureau of Statistics).*
Workers	Any person who receives payment for their work at LC (including part time, casual or full time).
Privacy	Information privacy is the right to have some control over how your personal information is collected and used. The Privacy Act allows individuals to request access to their personal information, know why information is being collected, how the information is being used, who the information will be disclosed to, request personal information to be adjusted if it is not correct, and how to make a complaint.
Policy	A policy is an overarching concise, definitive statement of direction, which is mandated and provides a framework for decision making. It demonstrates legislative compliance and strategic alignment

Procedure	A series of step by step instructions that outlines how an action should be implemented.
Volunteers	Volunteering is time willingly given for the common good and without financial gain. *Definition taken from Volunteering Australia*

34. RELEVANT DOCUMENTATION

34.1 Relevant Legislation

Commonwealth

- Australian Information Commissioner Act 2010 (Cth)
- Family Law Act 1975
- Family Law Amendment Act 2023
- Freedom of Information Act 1982 (Cth)
- National Disability Insurance Scheme Act 2013 (Cth)
    - National Disability Insurance Scheme (Code of Conduct) Rules 2018
    - National Disability Insurance Scheme (Quality and Safeguards Commission and other Measures) Act 2017
- Privacy Act 1988 (Cth)
- Privacy and Other Legislation Amendment Act 2024 (Cth)

State

- Care and Protection of Children Act 2007, (NT)
- Children and Young People (Safety) Act 2017 (SA)
- Freedom of Information Act 1991 (SA)
- Information Act, 2002 (NT)
- State Records Act 1997 (SA)
- Surveillance Devices Act 2016 (SA)
- Surveillance Devices Act 2002 (NT)

34.2 Overarching Codes / Frameworks

- Code of Fair Information Practice
- Information Privacy Principles (SA)
- Information Sharing Guidelines (SA)
- National Disability Insurance Scheme (Incident Management and Reportable Incidents) Rules 2018
- National Disability Insurance Scheme (Quality Indicators for NDIS Practice Standards) Guidelines 2018
- NDIS Practice Standards (specifically core module Section 1.3 and 2.4)
- NDIS Quality and Safeguarding Framework

34.3 Governance Policies / Standards

- Case Note Recording Policy
- Case Noting Practice Guide
- Child Safe Policy and Procedure
- Client Consent Policy – Elcies
- Client Incident Management Policy and Procedure
- Code of Conduct
- Elcies Incident Management Policy and Procedure
- Elcies Reportable Incidents involving the use of a Restricted Practice Policy and Procedure

- Employee Records Policy
- Feedback and Complaint Handling Policy
- ICT Data Breach Response Policy and Procedure
- Information and Communication Technology Policy and Procedure
- Information Sharing Guidelines (ISG) Procedures for Promoting Safety and Wellbeing in SA and NT
- Managing Unsatisfactory Performance and Conduct Policy and Procedure
- Misconduct Investigations Procedure
- Misconduct Policy
- Photograph and Video Footage Policy
- Process Map for handling client requests to access personal records
- Social Media Policy and Procedure
- Whistleblowers Policy and Procedure
- Workplace Surveillance Policy

34.4 Forms and Templates

- Client Authority to Disclose Information
- Client Consent to Information Sharing
- Client Consent form (NDIS only)
- Photographs and Video Consent
- Request for Access to Personal Records
- Use of Image Consent (Elcies)

35. APPROVAL

This policy and procedure has been approved by:

Name	Ashleigh Hosking
Delegate position	Executive Manager Services and Practice Quality
Date	9 June 2026
Signature