



Policy Name:	Privacy Policy
Attention:	All LSH Group Australia Employees
Version:	1.2
Last Reviewed:	1 st April 2026
Effective From:	1 st April 2026
Approved By:	GCEO / Corp Review / MD

Privacy Policy

1. Purpose

This policy sets out how LSH Group Australia collects, stores, uses, and discloses personal information in compliance with:

- *Privacy Act 1988 (Cth)* and *Australian Privacy Principles (APPs)*
- *Spam Act 2003 (Cth)*
- Relevant state privacy legislation in VIC, NSW, and QLD

The policy ensures personal information is handled responsibly, transparently, and securely, and outlines the obligations of employees in maintaining privacy.

2. Scope

This policy applies to all employees, contractors, and representatives of LSH Group Australia, covering personal information relating to:

- Customers
- Employees
- Suppliers, contractors, and other stakeholders

3. Definition of Personal Information

Personal information is any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in material form or not.

Examples include:

- Names, addresses, phone numbers
- Date of birth, identification numbers
- Employment, financial, or transaction records

Sensitive information (e.g., health, ethnicity, religious beliefs, union membership, political opinions) requires additional protection under the APPs.

4. Collection of Personal Information

Personal information must be collected only:

- For lawful purposes; and
- Where it is reasonably necessary for business functions or activities



Employees must ensure:

- Collection is fair and transparent
- The individual understands the purpose of collection and how the information will be used or disclosed
- Information is accurate, complete, and up to date
- Unnecessary or intrusive collection is avoided

Direct collection is preferred; collection from third parties is only permitted with consent or where authorised by law. For minors under 16, consent should be obtained from a parent or guardian.

5. Use and Disclosure

Personal information must be used and disclosed only:

- For the primary purpose of collection
- For a secondary purpose reasonably related to the primary purpose
- With the individual's consent
- Where required or authorised by law

Before use or disclosure, employees must take reasonable steps to ensure the information is:

- Accurate, complete, up-to-date, and relevant

Sensitive information requires explicit consent unless authorised by law.

Overseas disclosure (APP 8):

Before transferring personal information outside Australia, ensure:

- The recipient is subject to a comparable privacy law; or
- The individual has consented; or
- Disclosure is otherwise permitted under Australian law

6. Direct Marketing and Consent

All marketing communications must comply with the *Spam Act 2003*:

- Consent (express or implied) must be obtained before sending marketing communications
- Individuals must have a clear option to unsubscribe from communications
- Contact information must be accurate and not misleading

7. Data Security and Retention

LSH Group Australia will take reasonable steps to protect personal information against:

- Loss, misuse, interference, or unauthorised access
- Modification or disclosure

Employees must:

- Lock screens, log off computers, and secure workstations
- Use lockable storage for physical documents
- Dispose of unnecessary information securely (e.g., shredding, secure bins)
- Limit access to authorised personnel only



Personal information must not be retained longer than necessary for business or legal purposes.

8. Access and Correction

Individuals have the right to:

- Request access to their personal information
- Request correction to ensure accuracy and completeness

Requests must be processed promptly, reasonably, and without excessive cost.

9. Privacy Breach and Notifiable Data Breaches (NDB)

Employees must immediately report any suspected or actual privacy breaches to their Manager or Compliance Officer.

A privacy breach may include:

- Unauthorised access, disclosure, or loss of personal information

The Compliance Officer will:

- Assess the breach promptly
- Determine whether notification under the NDB scheme is required
- Notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when legally mandated
- Implement corrective actions to prevent recurrence

10. Employee Responsibilities

All employees must:

- Collect and handle personal information only when necessary
- Protect privacy and confidentiality
- Follow lawful directions regarding the storage, use, and disclosure of personal information
- Report suspected breaches promptly

Managers must ensure:

- Their team understands and complies with this policy
- Any privacy breaches are escalated and managed in accordance with this policy

The Compliance Officer / HR will oversee compliance, provide guidance, and coordinate breach responses.

11. Review

This policy will be reviewed periodically to ensure:

- Alignment with Australian legislation and APPs
- Compliance with Spam Act and NDB obligations
- Alignment with best practice privacy management

12. Key Principles for Employees



- Collect only what is necessary
- Be transparent about collection purposes
- Protect and securely store personal information
- Ensure information is accurate and up-to-date
- Provide access or corrections when requested
- Dispose of personal information securely when no longer required

13. Policy Status

This Policy does not form part of any employee's contract of employment. It is a lawful and reasonable direction of the Company with which compliance is required. Any statement in this Policy about what the Company will or will not do does not create a legally binding obligation on the Company.

This Policy may be amended from time to time to reflect changes in legislation, regulatory requirements or organisational needs.