

ICLRA Privacy Policy

Effective Date: 30/06/2026

Version: 1.0

Privacy Policy

The International Common Law Recognition Authority (ICLRA) ("ICLRA", "we", "our", or "us") is committed to protecting the privacy, dignity, confidentiality and security of every individual who engages with our organisation.

We recognise that those who interact with ICLRA often entrust us with highly sensitive personal information. We therefore maintain strict standards governing the collection, use, storage, disclosure and protection of that information.

This Privacy Policy explains how we collect, use, disclose, retain and protect information received through our websites, applications, membership services, education programs, certification processes, dispute resolution services, research activities and administrative operations.

1. Our Commitment

ICLRA is committed to:

- respecting every individual's right to privacy;
 - collecting only information reasonably necessary to perform our functions;
 - maintaining secure systems to protect information from unauthorised access;
 - ensuring confidentiality across all departments;
 - complying with applicable Australian privacy legislation where required; and
 - applying additional internal confidentiality standards where appropriate.
-

2. Who This Policy Applies To

This policy applies to information collected from:

- Members
- Applicants
- Students
- Graduates

- Volunteers
 - Staff
 - Contractors
 - Board members
 - Advisors
 - Elders
 - Assessors
 - Witnesses
 - Complainants
 - Respondents
 - Referees
 - Research participants
 - Donors
 - Website visitors
 - CRM users
 - Learning Management System users
 - Event attendees
 - Any individual interacting with ICLRA.
-

3. Information We Collect

Depending upon your interaction with ICLRA, we may collect:

Personal Information

Including but not limited to:

- Full name
 - Preferred name
 - Date of birth
 - Residential address
 - Postal address
 - Email address
 - Telephone numbers
 - Emergency contacts
 - Occupation
 - Employer
 - Educational history
 - Qualifications
 - Professional memberships
-

Identity Information

Where required, we may collect:

- Driver Licence
 - Passport
 - Birth Certificate
 - Government-issued identification
 - Citizenship or residency documentation
 - Working With Children Check
 - Police Checks
 - Professional registrations
-

Membership Information

Including:

- Membership class
 - Membership number
 - Status
 - Payment history
 - Renewal information
 - Voting eligibility
 - Committee appointments
-

Educational Records

Including:

- Enrolments
 - Course progress
 - Assessments
 - Certificates
 - Diplomas
 - Academic transcripts
 - Attendance
 - Learning records
 - Recognition of Prior Learning documentation
-

Applications

Where applications are submitted we may collect:

- Supporting documents
 - Statutory declarations
 - Evidence
 - References
 - Affidavits
 - Correspondence
 - Historical documentation
 - Genealogical records
 - Research materials
 - Photographs
 - Audio recordings
 - Video recordings
-

Sensitive Information

Some applications require information that may be considered sensitive.

Examples include:

- cultural heritage
- family history
- ancestry records
- compensation claims
- historical records
- legal proceedings
- witness statements
- financial hardship
- health information voluntarily provided
- disability information voluntarily provided
- trauma-related information
- other confidential evidence.

Sensitive information is only collected where reasonably necessary and, wherever practical, with consent.

Financial Information

Where required we may collect:

- Payment records
- Transaction history

- Donation history
- Invoice details
- Billing addresses

ICLRA does not store complete credit card details where payments are processed through secure third-party payment providers.

Website Information

When using our websites we may collect:

- IP address
 - Browser type
 - Device information
 - Operating system
 - Session information
 - Pages visited
 - Referral websites
 - Cookies
 - Analytics data
-

4. How We Collect Information

Information may be collected through:

- online forms
 - membership applications
 - education enrolments
 - CRM submissions
 - support requests
 - email correspondence
 - telephone conversations
 - meetings
 - interviews
 - video conferences
 - event registrations
 - surveys
 - website usage
 - cookies
 - payment gateways
 - referrals
 - publicly available sources where relevant
 - documents voluntarily submitted by applicants.
-

5. Why We Collect Information

Information is collected for purposes including:

- assessing applications;
 - verifying identity;
 - administering memberships;
 - delivering education and training;
 - issuing qualifications;
 - managing certifications;
 - processing payments;
 - maintaining member records;
 - communicating organisational updates;
 - conducting research;
 - administering dispute resolution;
 - managing complaints;
 - protecting organisational integrity;
 - complying with legal obligations;
 - improving services;
 - managing websites and digital platforms;
 - preventing fraud;
 - maintaining organisational security.
-

6. Legal Basis

Where applicable, information is collected because:

- you consent;
 - it is necessary to provide requested services;
 - it is required for contractual obligations;
 - it is required by law;
 - it is necessary for legitimate organisational administration.
-

7. Use of Information

Information will only be used for purposes consistent with those for which it was collected unless:

- you consent;
 - disclosure is authorised by law;
 - disclosure is necessary to protect safety;
 - disclosure is necessary to investigate fraud or unlawful conduct.
-

8. Confidential Information

Many matters managed by ICLRA involve highly confidential material.

Examples include:

- applications
- legal research
- historical investigations
- compensation matters
- governance records
- board discussions
- meeting recordings
- internal investigations
- policy development
- strategic planning
- financial planning
- security matters

Access is limited strictly to authorised personnel with a legitimate operational need operating under a current and valid Non-Disclosure Agreement.

9. Disclosure of Information

ICLRA does not sell personal information.

Information may be disclosed only where reasonably necessary to:

- authorised staff;
- authorised contractors;
- approved assessors;
- auditors;
- payment providers;
- learning management systems;
- website hosting providers;
- cloud storage providers;
- legal advisers;
- insurers;
- regulators where required;
- courts or tribunals where lawfully required.

All third-party providers are expected to maintain appropriate security standards.

10. International Disclosure

Some digital service providers may store information outside Australia.

Where this occurs, ICLRA endeavours to ensure providers maintain privacy protections substantially equivalent to Australian standards.

11. Data Security

ICLRA employs administrative, technical and physical safeguards including:

- encrypted connections (SSL/TLS)
- secure hosting
- firewall protection
- malware monitoring
- password protection
- role-based permissions
- multi-factor authentication where available
- regular software updates
- restricted administrative access
- audit logging
- secure backups
- confidentiality agreements
- staff training

Despite these measures, no electronic transmission can be guaranteed to be completely secure.

12. Data Retention

Information is retained only for as long as reasonably necessary to:

- fulfil organisational purposes;
- comply with legal obligations;
- maintain historical organisational records;
- preserve educational records;
- manage membership history;
- resolve disputes;
- protect organisational interests.

Some records of historical or organisational significance may be retained permanently.

13. Access to Your Information

You may request access to personal information we hold about you.

Requests should be submitted in writing.

Identity verification may be required before access is granted.

Access may be refused where permitted by law.

14. Correction of Information

If your personal information is inaccurate, incomplete or outdated, you may request correction.

Reasonable steps will be taken to update records promptly.

15. Withdrawal of Consent

Where information is collected by consent, you may withdraw consent unless retention is required by law or necessary to complete ongoing organisational processes.

Withdrawal of consent may affect our ability to provide certain services.

16. Cookies

Our websites may use cookies to:

- improve website performance;
- remember preferences;
- maintain login sessions;
- collect analytics;
- improve security.

Users may disable cookies through browser settings, although some website functions may be affected.

17. Marketing Communications

Members may receive:

- newsletters
- event notices
- education updates
- policy updates
- membership notices
- organisational announcements

Recipients may unsubscribe from non-essential communications at any time.

Important organisational notices may still be issued where necessary.

18. Children's Privacy

Where services involve minors, personal information should ordinarily be provided by or with the consent of a parent, guardian, or other authorised representative, unless otherwise permitted by law.

Additional safeguards may be applied where appropriate.

19. Research

Information may be used for research and statistical purposes.

Where possible:

- identifying information will be removed;
 - data will be aggregated; and
 - confidentiality will be maintained.
-

20. Website Security

We continuously monitor our systems to protect against:

- unauthorised access
- malware
- denial-of-service attacks
- spam

- data breaches
 - fraudulent activity
-

21. Data Breaches

If a data breach occurs that is likely to result in serious harm, ICLRA will take reasonable steps to:

- contain the breach;
 - investigate the incident;
 - notify affected individuals where appropriate;
 - comply with applicable legal notification obligations;
 - implement corrective measures.
-

22. Third-Party Websites

Our websites may contain links to external websites.

ICLRA is not responsible for the privacy practices of external organisations.

Users should review the privacy policies of those websites independently.

23. Changes to This Policy

This Privacy Policy may be amended from time to time.

Updated versions will be published on the ICLRA website together with the revised effective date.

Continued use of ICLRA services following publication constitutes acceptance of the updated policy.

24. Contact

Privacy Officer

International Common Law Recognition Authority (ICLRA)

Website: <https://iclraauthority.org>

Email: [Insert Privacy Email]

Postal Address: [Insert Postal Address]

25. Complaints

If you believe your privacy has been breached, please contact the Privacy Officer in writing.

We will acknowledge complaints promptly and endeavour to investigate and respond within a reasonable timeframe.

Where applicable under Australian law, individuals may also have the right to make a complaint to the Office of the Australian Information Commissioner (OAIC).

Acceptance

By submitting information to ICLRA, creating an account, applying for membership, enrolling in educational programs, making payments, submitting applications, or otherwise engaging with our services, you acknowledge that you have read, understood and accepted this Privacy Policy.