Pathway Learning Pty Ltd

Privacy Policy

Pathway Learning Pty Ltd

Last Updated: November 2025

About This Policy

This Privacy Policy explains how Pathway Learning Pty Ltd (ACN 689 734 656) collects, uses, discloses, holds and protects personal information. It applies to all personal information we collect from organisations, staff, volunteers, program participants, and other individuals who interact with us.
Pathway Learning Pty Ltd is bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) contained within it. This policy reflects our commitment to managing personal information openly and transparently.
For quick answers, see our Summary Privacy Statement. This full policy provides detailed information about our privacy practices.

1. Our Organisation Details

Organisation Name	Pathway Learning Pty Ltd
Email	privacy@pathwaylearning.au

2. What Personal Information Do We Collect?

Information We Collect Directly

When you interact with Pathway Learning Pty Ltd, we collect personal information you provide to us. This includes:
From Organisations and Contacts:

- Organisation name and legal entity details
- Contact person's full name, job title, and role
- Email address and phone number
- Organisation size, location, and sector
- Training interests and capacity-building priorities
- Governance and compliance challenges
- Budget information and funding sources
- Board structure and staff composition (when relevant to training design)

From Training Participants:

- Full name and employment title
- Email address and phone number (if provided)
- Department or team name
- Learning completion records
- Training feedback and assessment results
- Training attendance records
- Skill development tracking data

From Website Users:

- Name and contact details (if you submit a form)
- Messages and inquiries you send
- IP address and browsing behaviour (through analytics)
- Device type and operating system
- Pages visited and time spent on pages

From Volunteers and Staff (if applicable):

- Full name, date of birth, and gender
- Contact details (email, phone, address)
- Employment history and qualifications
- References and background check results
- Tax File Number (for payroll purposes)
- Bank account details (for payment purposes)

Information We Collect Indirectly

We may receive personal information about you from:

- Your organisation's leadership or designated training coordinator
- Third-party service providers who help us deliver training
- Publicly available sources (such as organisation websites or LinkedIn)
- Government agencies (if required by law)
- Other organisations referring you to Pathway Learning Pty Ltd

Information Collected Automatically

When you visit our website or use our training portal, we automatically collect:

- Your IP address
- Browser type and version
- Pages you visit and time spent on each page
- Links you click
- Referring website or search terms used
- Device information (type, model, operating system)
- Approximate location (city/country level, not precise)
- Login information (if you access our portal)

We collect this using cookies and analytics tools to understand how you use our website and improve your experience.

Payment Processing Information

When you make a payment for our training services, Stripe collects payment information on our behalf.
This includes:

- Payment card details (card number, expiration date, CVV code)
- Bank account details (if using direct debit)
- Billing name and address
- Transaction amount, date, and time
- Payment authorisation and confirmation details
- Device information and IP address used during payment

This information is collected directly by Stripe and is not stored on Pathway Learning Pty Ltd's systems. For complete details about payment information collection, see Section 5.1 Payment Processing and Stripe.

Sensitive Information

We do not routinely collect sensitive information. However, in limited circumstances, we may collect:

- Health information: Only if disclosed voluntarily during training context (e.g., accessibility needs)
- Religious or political affiliations: Only if relevant to your organisation's context or training needs and voluntarily disclosed
- Criminal records: Only if you apply for employment and voluntarily disclosed as part of background checks

We collect sensitive information only when it's directly relevant to our relationship with you and only with your clear consent.

3. Why Do We Collect and Use Your Information?

Primary Purposes

We use your personal information for these core purposes:

1. Delivering Training Services:
    - Understanding your organisation's capacity-building needs
    - Designing customised training programs
    - Delivering training content and materials
    - Managing training logistics (scheduling, venues, access)
    - Tracking participant progress and learning outcomes
    - Providing post-training support and resources
2. Communicating With You:
    - Responding to your inquiries
    - Sending you information about relevant training solutions
    - Notifying you of upcoming training programs
    - Providing training confirmations and calendar invitations
    - Sharing training materials and resources
    - Collecting feedback on training experiences
3. Administering Our Services:
    - Processing registrations and enrolments
    - Invoicing and payment collection
    - Maintaining training records and certifications
    - Delivering correspondence about your training
    - Managing our training portal and access
    - Complying with legal and contractual obligations
4. Improving Our Services:
    - Analysing how training is used and valued
    - Understanding organisational outcomes from training
    - Gathering feedback through surveys and evaluations
    - Identifying trends in capacity-building needs
    - Developing new training programs
    - Improving the quality of existing programs
5. Research and Insights (with consent):
    - Understanding capacity-building trends in the NGO sector
    - Publishing anonymised case studies (with your permission)
    - Contributing to broader sector understanding of effective training
    - Demonstrating impact of training interventions
6. Legal and Compliance:
    - Complying with Privacy Act obligations
    - Responding to law enforcement requests
    - Protecting our legal rights
    - Maintaining audit trails and regulatory compliance
7. Direct Marketing (only with consent):
    - Sending you information about new training programs
    - Inviting you to events or webinars
    - Sharing sector insights and resources
    - Offering special pricing or early-bird discounts

Legal Bases for Processing

We process your information under these legal bases:

- Contractual necessity: Information required to fulfill training agreements with you
- Legal obligation: Information required by Australian law (Privacy Act, employment law, tax law)
- Legitimate interests: Information needed to improve our services and understand training effectiveness
- Your consent: Information you've explicitly agreed we can use for specific purposes

- Compliance with law: Information required by government agencies or regulatory authorities

Information We Don't Use

We will never:

- Sell your personal information to third parties
- Use your information for purposes unrelated to training and organisational capacity-building
- Share your information with marketing companies or telemarketers
- Use your information to make automated decisions about you (without human review)
- Use your sensitive information without explicit consent

4. How Do We Hold and Protect Your Information?

Data Security Measures

We take your privacy seriously and implement comprehensive security measures:
Technical Security:

- Encryption: All data transmitted to and from our portal uses SSL/TLS encryption (indicated by "https" in your browser)
- Access controls: Staff access personal information only when needed for their role
- Multi-factor authentication: Multiple layers of verification for portal access
- Regular security updates: Software and systems updated regularly to address security vulnerabilities
- Firewalls and intrusion detection: Monitoring systems to detect unauthorised access attempts
- Data backups: Regular encrypted backups to prevent data loss
- Secure deletion: When information is no longer needed, we use secure deletion methods to prevent recovery

Organisational Security:

- Privacy training: All staff receive training on privacy obligations and data handling practices
- Access restrictions: Personal information restricted to authorised staff only
- Visitor policies: Controlled access to physical premises
- Incident response plan: Established procedures for responding to data breaches
- Regular audits: Annual reviews of our information handling practices
- Vendor management: Third-party providers assessed for security and privacy compliance

Password and Account Security:

- We recommend using strong, unique passwords
- We encourage enabling two-factor authentication where available
- Change your password regularly
- Don't share your portal login with others
- Contact us immediately if you suspect unauthorised access

Data Retention and Deletion

We keep personal information only for as long as it's needed:

Type of Information	Retention Period	Reason
Training registrations and attendance	7 years	Legal/regulatory compliance and training records
Learning outcomes and assessments	7 years	Training effectiveness and organisational records
Contact information for active clients	Duration of relationship + 1 year	Client relationship management
Contact information for inactive organisations	12 months	Regulatory compliance and re-engagement

Type of Information	Retention Period	Reason
Website analytics data	12-24 months	Service improvement and trend analysis
Email inquiries	12 months	Customer service records
Staff/volunteer records	7 years after employment ends	Legal compliance and reference purposes
Payment and financial records	7 years	Tax and accounting requirements
Data breach records	As per legal requirements	Regulatory compliance

Deletion Process:

- When information is no longer needed, we securely delete it
- Deletion involves secure data destruction that prevents recovery
- We may retain anonymised data for research and trend analysis
- We comply with your requests for deletion (subject to legal obligations)

Your Right to Request Deletion:

You can request deletion of your personal information at any time by emailing privacy@pathwaylearning.au. We'll respond within 30 days. We may need to retain information if required by law, to complete your training, or to fulfill contractual obligations.

5. Who Do We Share Your Information With?

Organisations We Share Information With

We share your personal information with limited, trusted partners necessary to deliver our services:

Essential Service Providers:

Provider Type	Purpose	Information Shared
Cloud Storage/Portal Provider	Hosting our training portal and materials	Training registrations, progress, learning data
Email Service Provider	Sending training notifications and correspondence	Name, email address, training schedule
Analytics Provider	Understanding website usage and optimisation	IP address, browsing behaviour, page visits
Learning Management System (LMS)	Delivering online training content	Name, email, training progress, assessments
Payment Processor (Stripe, Inc.)	Processing online payments, preventing fraud, handling disputes and chargebacks, complying with financial regulations	Name, email, organisation name, billing address, payment card details (card number, expiration, CVV), bank account details, transaction amounts and dates, IP address and device information
Video Conferencing Provider	Delivering online or hybrid training	Name, email, organisation, video/audio during sessions

All service providers are contractually required to:

- Comply with Australian Privacy Act and APPs
- Use information only for the purposes we specify
- Maintain appropriate security measures
- Delete information when no longer needed

- Not disclose information to third parties

When We Might Share Information Without Consent

In limited circumstances, we may disclose information without consent:

- Law enforcement or government request: If required by law, court order, or legitimate government authority
- Legal proceedings: If necessary to protect our legal rights or respond to litigation
- Serious harm prevention: If disclosure is necessary to prevent serious physical harm to an individual
- Regulatory investigations: If responding to investigations by privacy authorities or regulators
- Merger or sale: If our organisation is acquired, information may transfer to the new owner (you'll be notified)

Information We Don't Share

We will not share your information with:

- Marketing agencies or telemarketers
- Data brokers or list sellers
- Political parties or advocacy groups
- Competitors or other NGOs
- Your organisation's funders (without explicit agreement)
- Media or public relations agencies
- Any third party without your consent (except as required above)

Payment Processing and Stripe

How We Process Payments

Pathway Learning Pty Ltd uses Stripe, Inc. ("Stripe") as our third-party payment processor to securely process online payments for training services. When you make a payment through our website or training portal, your payment information is collected and processed by Stripe.
Stripe operates independently from Pathway Learning Pty Ltd and is responsible for the security and handling of your payment data in accordance with international payment security standards.

What Information Stripe Collects

When you make a payment through our website or training portal, Stripe collects:

- Your name and email address – To identify the purchaser and send payment confirmations
- Billing and shipping address – To verify payment method and prevent fraud
- Payment method details – Credit/debit card number, expiration date, CVV code, or bank account details for direct debit
- Transaction information – Transaction amount, date, time, currency, and description of services purchased
- Device and connection information – IP address, browser type, operating system, and device information for fraud prevention and security
- Organisation name – When purchasing on behalf of an organisation, for invoicing purposes

Pathway Learning Pty Ltd does not store your complete payment card details on our systems. This information is securely collected and held by Stripe in compliance with Payment Card Industry Data Security Standards (PCI DSS Level 1).

Stripe's Role as Independent Data Controller

It's important to understand that Stripe acts as an independent data controller for payment transaction data. This means:

- Stripe determines how your payment information is processed – Stripe has its own data handling policies and procedures
- Stripe is responsible for securing your payment data – Stripe maintains industry-leading security measures for payment information
- Stripe's Privacy Policy governs Stripe's use of your information – Stripe's handling of your payment data is subject to Stripe's own privacy commitments
- You can review Stripe's Privacy Policy at: https://stripe.com/privacy

While Pathway Learning Pty Ltd remains accountable under Australian Privacy Principles for choosing Stripe as our payment processor, Stripe independently manages the security and processing of your payment information.

Why We Share Your Information with Stripe

We share your information with Stripe for the following purposes:

- Process your payment securely and efficiently – To complete transactions for training services you've purchased
- Prevent fraudulent transactions – To protect you and Pathway Learning Pty Ltd from payment fraud and unauthorised transactions
- Comply with financial regulations – To meet anti-money laundering requirements and other financial compliance obligations
- Fulfill our contractual obligations – To provide the training services you've paid for
- Issue invoices and receipts – To provide documentation of your transactions for your records
- Handle payment disputes and chargebacks – To manage any issues that arise with your payment
- Process refunds – To return payments when required under our Refund Policy or Terms and Conditions

Your payment information is shared with Stripe only for these legitimate payment processing purposes and is not used by Pathway Learning Pty Ltd for any other purpose.

Stripe's Security Measures

Stripe maintains the highest levels of payment security:

- PCI DSS Level 1 Certification – The highest level of payment card security certification, verified annually
- Industry-leading encryption protocols – All payment data is encrypted during transmission and storage using AES-256 encryption
- Fraud detection and prevention systems – Advanced machine learning algorithms monitor transactions for suspicious activity
- Secure tokenisation – Payment card details are converted to secure tokens that cannot be reverse-engineered
- Compliance with international payment standards – Stripe complies with payment security requirements across multiple jurisdictions
- Regular security audits – Independent third-party security assessments conducted regularly
- 24/7 security monitoring – Continuous monitoring for security threats and anomalies

Stripe's security infrastructure is designed to protect your payment information from unauthorised access, loss, misuse, and disclosure.

Overseas Disclosure Through Stripe

Stripe, Inc. is headquartered in San Francisco, California, United States of America.
When you make a payment through our website:

- Your payment information is transmitted to Stripe's servers in the United States – This occurs in real-time during payment processing
- Stripe processes payments through its global infrastructure – Stripe may process your information through servers located in the United States, European Union, Singapore, and other jurisdictions
- Cross-border data transfer protections – Stripe complies with the Data Privacy Framework (formerly EU-US Privacy Shield) and other international data protection frameworks
- Pathway Learning Pty Ltd remains accountable – Under Australian Privacy Principle 8 (APP 8), we remain responsible for Stripe's handling of your payment information and have taken steps to ensure Stripe provides appropriate protections

Why Overseas Disclosure Is Necessary

Overseas disclosure to Stripe is necessary because:

- Stripe's payment processing infrastructure operates globally to provide fast, secure, and reliable payment processing
- International payment networks (Visa, Mastercard, etc.) require processing through global systems
- Fraud prevention systems analyse transaction patterns across multiple jurisdictions
- No equivalent Australian-only payment processor can provide the same level of security, reliability, and payment method diversity

Your Rights Regarding Payment Information

You have the following rights regarding your payment information:
Access: You can request access to your payment transaction history by:

- Logging into your Pathway Learning Pty Ltd portal account to view your transaction history
- Contacting us at privacy@pathwaylearning.au to request a copy of your payment records
- Contacting Stripe directly at https://support.stripe.com/ regarding payment data held by Stripe

Correction: If your billing information is inaccurate or has changed, you can:

- Update your billing information in your portal account settings
- Contact us at privacy@pathwaylearning.au to request correction of billing details
- Contact your financial institution to update payment method information

Deletion: You can request deletion of your payment history, subject to:

- Legal requirements to retain financial records for 7 years for tax and accounting purposes
- Contractual obligations to maintain records of services provided and payments received

Stripe's own data retention requirements for fraud prevention and regulatory compliance

After legal retention periods expire, we will securely delete your payment information upon request.
Dispute Payment Processing: If you believe a payment was processed incorrectly, you can:

- Contact us at privacy@pathwaylearning.au within 60 days of the transaction
- Lodge a dispute through your financial institution (chargeback process)
- Contact Stripe directly at https://support.stripe.com/ regarding payment processing issues

Withdraw Consent for Future Payments: You can choose not to make future payments through Stripe, though this will prevent you from purchasing additional training services online. Alternative payment arrangements may be discussed by contacting us directly.

Stripe's Contact Information

If you have questions or concerns specifically about how Stripe handles your payment information:

- Email: privacy@stripe.com
- Website: https://stripe.com/privacy
- Customer Support: https://support.stripe.com/
- Australian Business Address: Stripe is registered in Australia and operates under Australian company registration

For questions about your payments to Pathway Learning Pty Ltd or billing inquiries, please contact us directly at privacy@pathwaylearning.au or the contact details in Section 16 of this Privacy Policy.

6. Overseas Disclosure of Personal Information

Will We Disclose Information Overseas?

Unlikely: We primarily operate within Australia and store information on Australian servers.
If overseas disclosure occurs, it may involve:

- Cloud service providers: Some cloud infrastructure providers operate globally. We use providers with Australian data centers where possible
- Third-party partners: If we work with international training organisations or developers
- Your organisation's request: If you request information be shared with overseas partners

Where Overseas Recipients Are Located

If information is disclosed overseas, it may go to:

- United States (Stripe Payment Processing): Our payment processor Stripe, Inc. is headquartered in San Francisco, California, USA and processes all payment transactions through its global infrastructure located in the United States, European Union, Singapore, and other jurisdictions. Stripe complies with the Data Privacy Framework for cross-border data transfers and maintains PCI DSS Level 1 certification (the highest level of payment card security). We remain accountable for Stripe's handling of your payment information under Australian Privacy Principle 8 (APP 8). When you make a payment, your payment card details, billing information, transaction data, and device information are transmitted to and stored on Stripe's secure servers overseas. For complete details about Stripe's data processing and your rights, see Section 5.1.
- European Union countries (data protection-focused providers)
- Other countries where our service providers operate

Your Consent for Overseas Disclosure

If we need to disclose your information overseas, we will:

- Notify you in advance
- Obtain your consent before proceeding
- Ensure the recipient has adequate privacy protection (equivalent to Australian standards where possible)
- Remain responsible for the recipient's handling of your information

Your Right to Object

You can ask us not to disclose your information overseas by emailing privacy@pathwaylearning.au. We'll work with you to find alternative arrangements.

7. How Can You Access and Correct Your Information?

Your Right to Access

You have the right to request access to personal information we hold about you. To request access:
Email:
privacy@pathwaylearning.au
In Your Request, Include:

- Your full name
- The organisation you're affiliated with
- Specific information you're requesting
- Brief explanation of what you need the information for
- Preferred format (electronic, printed, etc.)

Our Response Timeline:

- We aim to respond within 10 business days
- Complex requests may take up to 30 days
- We'll notify you if access will take longer
- We may ask clarifying questions if your request is unclear

Access Fees:

- Most access requests are provided free of charge
- If your request is complex and requires significant resources, we may charge a reasonable fee (we'll notify you in advance)

Your Right to Correction

If your personal information is inaccurate, incomplete, or out of date, you can request we correct it.
How to Request Correction:
Email: privacy@pathwaylearning.au
Include in Your Request:

- The information you believe is incorrect
- What the correct information should be
- Supporting documentation if available

Our Correction Process:

- We'll investigate your request promptly
- If we agree the information is incorrect, we'll correct it
- If we disagree, we'll explain our decision and your right to complain
- We'll notify you once correction is complete
- If we've disclosed the incorrect information to others, we'll notify them of the correction (where practicable)

What If You Disagree?

If you disagree with our decision on correction, you have the right to:

- Ask us to note your disagreement on your record
- Lodge a complaint with the Office of the Australian Information Commissioner (see Section 9)

8. Your Privacy Rights and Choices

Opting Out of Communications

Marketing Communications:
If you no longer wish to receive information about training programs and services, you can:

- Click "unsubscribe" on any email we send
- Contact us: privacy@pathwaylearning.au
- Request removal from our mailing list

We'll honour your request within 5 business days.
Important Note: You cannot opt out of essential communications related to:

- Training you've enrolled in
- Contractual obligations and invoicing
- Legal compliance requirements
- Response to your inquiries

Managing Cookies and Analytics

Browser Controls:
Most browsers allow you to control cookies. You can:

- Disable cookies entirely
- Allow only certain cookies
- Delete cookies after each session

Visit your browser settings for instructions.

Opting Out of Analytics

If you don't want us to collect analytics data about your website:

- Install browser extensions that block analytics tracking

Withdrawing Consent

If you've consented to specific uses of your information (like research or marketing), you can withdraw that consent anytime by emailing privacy@pathwaylearning.au. Withdrawal will take effect going forward (we'll continue to use information for purposes already undertaken).

Opting Into Additional Services

Some uses of your information require your explicit consent, including:

- Sharing de-identified case studies in our marketing
- Asking you to participate in research about training effectiveness
- Inviting you to participate in sector research projects

You can opt into any of these by contacting privacy@pathwaylearning.au or selecting relevant options in our portal.

9. Privacy Complaints and How to Resolve Them

How to Make a Privacy Complaint

If you believe we've breached the Australian Privacy Principles or this policy:
Step 1: Contact Us
Email your complaint to: privacy@pathwaylearning.au
Include in Your Complaint:

- Your full name and contact details
- Description of the privacy concern
- What we allegedly did wrong
- When the incident occurred
- How it has affected you
- What resolution you're seeking

- Any supporting documentation

Step 2: Our Investigation

We will:

- Acknowledge your complaint within 5 business days
- Investigate thoroughly and promptly
- Keep you informed of progress
- Respond with a detailed explanation within 30 days (or 45 days for complex matters)
- Explain the resolution and your rights if dissatisfied

Office of the Australian Information Commissioner (OAIC)

If you're not satisfied with our response, or if we don't respond within 30 days, you can lodge a formal complaint with:

Office of the Australian Information Commissioner

- Website: www.oaic.gov.au
- Email: enquiries@oaic.gov.au
- Phone: 1300 363 424
- Mail: GPO Box 3131, Canberra ACT 2601

The OAIC will:

- Investigate your complaint independently
- Help resolve privacy disputes
- Potentially investigate our practices
- Take regulatory action if warranted

You can lodge a complaint with OAIC for free.

10. Data Breaches: What Happens If Your Information Is Compromised?

What Is a Data Breach?

A data breach occurs when your personal information is accessed, used, or disclosed without authorisation in a way that is likely to result in serious harm.

Our Breach Response Process

Immediate Response (upon discovery):

1. Contain and stop the breach
2. Assess the extent of the breach
3. Identify affected individuals
4. Prevent further unauthorised access

Assessment (within 30 days):

1. Determine if notification is required
2. Assess likelihood of serious harm
3. Evaluate whether remedial action can reduce harm
4. Document findings

Notification (if required):

If your information is involved in a breach that could cause serious harm:

- We'll notify you directly within 30 days of assessment
- We'll notify the OAIC
- We may make a public statement if individuals can't be identified

Your Notification Will Include:

- Description of what happened
- What information was affected
- Steps we're taking to remediate
- What you should do to protect yourself
- How to contact us for more information

You Have the Right to Know

You can request information about data breaches affecting you by emailing privacy@pathwaylearning.au.

11. Privacy Policy Updates

When We Update This Policy

We review and update this policy regularly to reflect:

- Changes to our information handling practices
- New regulatory requirements
- Feedback from privacy complaints
- Technological developments
- Sector best practices

How We'll Notify You

Website: We'll update the "Last Updated" date at the top of this policy
Material Changes: If the changes significantly affect your privacy, we'll email you or post a notice on our website
Your Right to Review: You can always request a copy of previous versions of our policy

12. Privacy by Design and Impact Assessments

How We Protect Privacy From the Start

We embed privacy into how we design our services:

- Privacy by design: Privacy considered in all new systems and processes
- Privacy impact assessments: Regular reviews of practices that handle sensitive information
- Staff training: All team members trained on privacy obligations
- Regular audits: Annual reviews of compliance with this policy and Australian Privacy Principles

13. Accountability and Governance

Our Privacy Management Framework

We maintain:

- Privacy policy (this document)
- Privacy management plan: Actions to maintain APP compliance
- Privacy incident response plan: Procedures for responding to breaches
- Staff privacy training: Annual training for all team members
- Privacy register: Log of privacy complaints and outcomes
- Data retention schedule: Guidelines for how long we keep information

Our Privacy Officer

Our Privacy Officer is responsible for:

- Overseeing compliance with this policy
- Investigating privacy complaints
- Implementing privacy improvements
- Liaising with the OAIC

Contact: privacy@pathwaylearning.au

14. Specific Information for Different Audiences

For Organisations Registering for Training

When your organisation registers with Pathway Learning Pty Ltd:

- We use your information to design relevant training and communicate about your programs
- We may de-identify your organisation to use as a case study (with permission)
- We retain your information to maintain our relationship and for training records
- You can request deletion of your information at any time

For Training Participants

When you participate in our training:

- We track your attendance and learning progress
- We collect feedback to improve programs
- We may use de-identified completion data in sector research
- Your learning records are maintained for 7 years for training certification purposes
- You can access your own learning records anytime

For Website Visitors

When you visit our website:

- We collect analytics to understand how people use our site
- You can opt out of analytics tracking
- We don't identify individuals unless you submit a form
- Cookies are used to improve your experience
- You control your own cookie settings through your browser

For Job Applicants and Employees

When you apply for a position or work with us:

- We collect information necessary to assess your suitability
- Background checks may include criminal record information (with consent)
- Employment records are maintained for 7 years after employment ends
- You have access rights to your employment file
- You have privacy protections under employment law

15. General Privacy Information

Australian Privacy Principles (APPs)

Our practices comply with all 13 Australian Privacy Principles, which address:

APP	Focus	Our Commitment
APP 1	Open and transparent management	Clear, accessible privacy policies
APP 2	Anonymity and pseudonymity	Option to use pseudonyms where practicable
APP 3	Collection of solicited personal information	Collect only necessary information
APP 4	Dealing with unsolicited personal information	Destroy information we don't need
APP 5	Notification of collection	Tell you when we collect information
APP 6	Use and disclosure	Use information only for stated purposes

APP	Focus	Our Commitment
APP 7	Overseas disclosure	Minimise overseas disclosure, obtain consent
APP 8	Transparency about third parties	Tell you about service providers
APP 9	Adoption, use or disclosure of government identifiers	Don't use government IDs unnecessarily
APP 10	Quality of personal information	Keep information accurate and up to date
APP 11	Security of personal information	Implement appropriate security measures
APP 12	Access and correction	Provide access to your own information
APP 13	Correction of personal information	Let you correct inaccurate information

Legislative Compliance

We comply with:

- Privacy Act 1988 (Cth)
- Notifiable Data Breaches (NDB) Scheme
- Privacy and Other Legislation Amendment Act 2024 (Cth)
- Australian Privacy Principles (APPs)
- Relevant State and Territory privacy laws

16. Contact Us

Privacy Questions or Concerns?

We're happy to discuss our privacy practices and address any concerns.
Contact Information:

Method	Details
Email	privacy@pathwaylearning.au
Response Time	Within 5 business days

17. Summary: Your Privacy Rights at a Glance

Right	What It Means
Know what we collect	You have the right to understand what personal information we hold
Access your information	You can request to see personal information we hold about you
Correct inaccurate information	You can ask us to fix information that's wrong or outdated
Request deletion	You can ask us to delete your information (subject to legal requirements)
Limit direct marketing	You can ask us not to send you marketing communications
Understand overseas disclosure	You should be told if your information goes overseas

Right	What It Means
Opt out of analytics	You can choose not to have your website use tracked
Withdraw consent	You can take back consent you've given for specific uses
File a complaint	You can complain if you believe we've breached your privacy
Know about breaches	You should be notified if a data breach affects your information

18. Glossary of Terms

Australian Privacy Principles (APPs): 13 principles that govern privacy in Australia, contained in the Privacy Act.
Consent: Your voluntary, informed agreement to how we collect, use, or disclose your information.
Data breach: Unauthorised access, use, or disclosure of personal information that could cause serious harm.
Disclosure: When we share or provide personal information to another person or organisation.
Eligible data breach: A data breach that meets the criteria for mandatory notification under Australian law.
Encryption: Technical security process that converts information into unreadable code that protects it from unauthorised access.
Multi-factor authentication: Security method requiring two or more forms of verification to access an account.
OAIC: Office of the Australian Information Commissioner, the regulator responsible for enforcing Australian privacy law.
Personal information: Information about an identified individual or an individual who can be reasonably identified.
Privacy Impact Assessment: Review of information handling practices to identify privacy risks and protections needed.
Pseudonym: A fictitious name used instead of your real name.
Sensitive information: Information about an individual's racial or ethnic origin, political opinions, religion, trade union membership, criminal record, or health information.
Third party: A person or organisation other than you and us.

19. Document History and Version Control

Version	Date	Key Changes
1.0	November 2025	Initial Privacy Policy for Pathway Learning Pty Ltd. Incorporates all APP 1 requirements Addresses 2024/2025 privacy law amendments Includes notifiable data breach obligations

Questions About This Policy?

If anything in this policy is unclear or you'd like to discuss your privacy with us, please don't hesitate to contact our Privacy Officer at privacy@pathwaylearning.au.
We're committed to protecting your privacy and building trust through transparent, respectful information handling practices.
Pathway Learning Pty Ltd is committed to supporting NGO capacity building while protecting the privacy and personal information of all organisations and individuals we work with.