

# MindBridge Education

## *Privacy Policy*



Prepared by:  
MindBridge Team  
MindBridge Education  
Brisbane, Queensland  
March 2025  
[www.mindbridgeedu.com.au](http://www.mindbridgeedu.com.au)



## 1. Introduction

### Purpose of This Policy

This Privacy Policy is intended to clearly outline how MindBridge Education ("MindBridge", "we", "our", "us") collects, uses, discloses, and manages personal information in accordance with its legal obligations. The policy applies to all individuals who engage with our services, including students, parents/guardians, employees, contractors, and website visitors.

MindBridge is committed to safeguarding personal privacy and is dedicated to being transparent about how personal information is handled. This document aims to provide a clear understanding of the rights individuals have in relation to their personal data and how they can exercise those rights.

By accessing or using our services—including tutoring sessions, school programs, communications, website forms, or any interactions with MindBridge—you agree to the terms outlined in this policy.

### Company Identity

MindBridge Education is an Australian educational organisation based in Queensland, offering structured, school-based academic support programs tailored to improve student outcomes. Our services are designed for students seeking personalised, high-impact academic support delivered by high-achieving university mentors. We work in direct partnership with schools and families across Queensland.

We are committed to operating with integrity, professionalism, and full respect for the confidentiality of all individuals we serve.

### Contact Details

#### MindBridge Education Pty Ltd

Brisbane, Queensland

Email: [info@mindbridgeedu.com.au](mailto:info@mindbridgeedu.com.au)

Phone: 0414082007

### Legal Compliance

MindBridge is bound by the Privacy Act 1988 (Cth) and is fully committed to complying with the Australian Privacy Principles (APPs), which govern the way personal information is collected, used, stored, and disclosed. These principles apply to all personal information we gather in both physical and digital environments.

Our commitment to compliance includes:

- Transparency about the types of data collected and the reasons for doing so.
- Clear procedures for gaining consent before collecting or using sensitive information.
- Secure storage and restricted access to personal data.
- Prompt response to data breach incidents and formal complaints.
- Allowing individuals to access, update, or correct their personal data upon request.

This policy will be reviewed and updated regularly to ensure it remains aligned with legal requirements and best practices.

## 2. What Kinds of Personal Information Does MindBridge Collect?

MindBridge Education collects and holds a range of personal information to deliver high-quality academic services, comply with legal obligations, and support effective communication with students, parents, staff, and schools. The types of information we collect depend on your interaction with us but always align with the principles of necessity, transparency, and consent.



## 2.1 Information We Collect From Students and Parents/Guardians

When enrolling in our programs or engaging with our services, we may collect the following types of personal information:

- **Full name** of student and parent/guardian
- **Date of birth** and **age** of the student
- **Contact details**, including address, email, and phone number
- **School name**, year level, and academic background
- **Academic performance records** (e.g. grades, progress reports)
- **Behavioural notes** or study concerns raised by the school or parents
- **Learning preferences or needs**, including details of learning difficulties, disabilities, or additional support requirements
- **Emergency contact information**
- **Health information** relevant to participation in the program (e.g., allergies, conditions that may affect attendance or learning)

We collect this information directly from the parent/guardian or student through enrolment forms, communications, or during school-based interactions.

## 2.2 Information We Collect From Tutors, Staff, and Job Applicants

For individuals applying to work or currently employed by MindBridge, we may collect:

- **Full name, address, and contact information**
- **Educational background and qualifications**
- **Academic transcripts and ATAR scores**
- **Employment history** and references
- **Working With Children Check (Blue Card)** and criminal history checks
- **Tax File Number (TFN)** and **bank details** (for payroll purposes)
- **Superannuation information**
- **Availability and scheduling preferences**
- **Emergency contact details**

Some of this information may be considered **sensitive** and is handled with additional care and only collected with the applicant's express consent.

## 2.3 Sensitive Information

Sensitive information is a special category of personal data which includes:

- Health or medical information
- Racial or ethnic origin
- Religious beliefs
- Criminal history
- Gender identity or sexuality
- Disability status

MindBridge will only collect sensitive information:

- When it is **reasonably necessary** for our operations (e.g. health conditions that impact tutoring sessions)
- When **express consent** is provided by the individual or their legal guardian
- When **required or authorised by law**, court orders, or regulatory bodies

## 2.4 Personal Information from Schools

With consent, MindBridge may collect or receive personal information about students directly from school staff or school databases. This could include:

- Enrolment status or year level
- Learning plans or Individual Education Plans (IEPs)
- Attendance or behavioural notes



- Academic goals or feedback from teachers

This information allows us to personalise tutoring and track student progress while working collaboratively with school partners.

### 2.5 Anonymous Interaction

Where it is lawful and practical, individuals may choose to interact with MindBridge anonymously (e.g., general inquiries). However, this may limit our ability to provide specific services (e.g., enrolment, school reporting, or academic support).

## 3. How MindBridge Uses Personal Information

MindBridge Education uses personal information only for purposes that are directly related to our core educational services, regulatory obligations, operational efficiency, and student safety. We are committed to transparency and minimising any risk of misuse by clearly defining how and why we collect, use, store, and disclose personal data.

This section outlines the key purposes for which MindBridge processes personal information and the legal basis for doing so.

### 3.1 Primary Purpose of Collection

The **primary purpose** for collecting personal information is to provide high-quality tutoring, educational support, and school partnership services. Specifically, this includes:

- Enrolling students into programs
- Scheduling and administering tutoring sessions
- Monitoring student progress and tailoring instruction
- Communicating with parents, schools, and students
- Managing school relationships and reporting outcomes
- Ensuring student safety and wellbeing during on-site sessions
- Staffing and payroll operations
- Maintaining secure and effective internal systems
- Meeting all legal and regulatory requirements

Personal information is only used for the primary purpose for which it was collected unless an individual provides consent for another use or the alternative use is permitted by law.

### 3.2 Secondary Purposes (Within Reasonable Expectations)

MindBridge may also use personal information for **secondary purposes** that are directly related to the primary purpose and within the individual's reasonable expectations. These include:

- Internal record-keeping and auditing
- Training and mentoring tutors (using anonymised academic case studies)
- Improving the design and delivery of educational programs
- Handling inquiries, feedback, and complaints
- Evaluating program effectiveness and learning outcomes
- Conducting risk assessments, safety checks, and health disclosures

These uses help MindBridge continuously improve its services and meet school and parent expectations without requiring fresh consent every time.

### 3.3 Use for Direct Marketing (With Consent)

MindBridge may use contact details to send updates about our services, educational resources, and program offerings to enrolled families or interested parties. This includes:

- Newsletters
- Event invitations
- Announcements of new programs or courses
- Campaigns promoting enrolment or educational initiatives

Marketing content is only sent:



- With express or implied **consent** from the recipient
- Where an **opt-out** option is always available and clearly communicated

MindBridge will **never** sell or rent personal information to external marketing providers.

### 3.4 Use in Program Reporting and Collaboration With Schools

Where MindBridge delivers on-site services in partnership with schools, personal and academic data may be used for:

- Tracking attendance and session completion
- Reporting learning progress to teachers
- Flagging academic or behavioural concerns
- Aligning tutoring content with in-classroom curriculum

In such cases, only relevant and necessary information is shared with school personnel in compliance with school agreements and student privacy expectations.

### 3.5 Use in Employment and Contractor Management

MindBridge uses the personal information of employees, tutors, and contractors for:

- Recruitment and vetting processes
- Conducting Blue Card and background checks
- Employment contracts and records
- Payroll and superannuation administration
- Allocating sessions and tracking tutor availability
- Managing performance, training, and compliance

All employment data is stored securely and only accessed by authorised internal personnel.

### 3.6 Lawful and Emergency Use

MindBridge may use or disclose personal information **without consent** in cases where:

- It is necessary to **protect the life, health, or safety** of any individual (e.g., medical emergencies during tutoring sessions)
- It is required or authorised by **Australian law, court, or tribunal order**
- It is necessary to **prevent, detect or respond to unlawful activity**, suspected fraud, or serious misconduct
- A **regulatory authority or law enforcement agency** requests access as part of a lawful investigation

Such disclosures are documented internally and only made when strictly justified

## 4. Disclosure of Personal Information

MindBridge Education may disclose personal information only when it is necessary for delivering services, fulfilling legal obligations, or protecting student safety. We do **not sell, rent, or share personal information with third parties** for commercial purposes. All disclosures are strictly controlled, recorded, and governed by applicable privacy laws and contractual obligations.

This section explains when and to whom MindBridge may disclose personal data, and what steps are taken to ensure its protection.

### 4.1 Who May Receive Disclosures

MindBridge may disclose personal information to the following **authorised and relevant parties**, where required:

- **Partner Schools** – for attendance tracking, progress reporting, behavioural alerts, learning adjustments, and emergency contact purposes
- **Parents/Guardians** – to communicate session updates, academic progress, or incidents
- **Medical Professionals** – in urgent circumstances involving the safety, health, or wellbeing of a student or staff member
- **Tutors and Staff** – on a strictly need-to-know basis to deliver tailored learning support



- **Legal and Regulatory Bodies** – such as the Office of the Australian Information Commissioner (OAIC), if required by law or under a formal investigation
- **Third-party Service Providers** – such as IT support, payment processors, learning platforms, cloud services or background screening agencies (e.g., Blue Card Services), only where these providers are under strict confidentiality and data protection agreements
- **Insurers and Legal Advisers** – in the event of a legal dispute, insurance claim, or compliance audit
- **Police and Child Protection Authorities** – in situations where a disclosure is legally mandated or in the best interests of the child's safety (e.g., suspected abuse, threats of harm, or criminal activity)

## 4.2 Conditions for Disclosure

All disclosures are governed by the following safeguards:

- **Minimum Necessary Disclosure** – only the data required for the specific purpose is shared; unnecessary details are withheld.
- **Need-to-Know Basis** – only individuals or organisations with a direct role in the matter can access the data.
- **Strict Third-Party Contracts** – external parties must enter into binding privacy agreements that comply with the Privacy Act 1988 (Cth) and the Australian Privacy Principles.
- **No International Transfers Without Safeguards** – personal data is not transferred outside Australia unless the recipient country has equivalent privacy protections, or the data is encrypted and anonymised in transit.
- **Written Consent for Unusual Disclosures** – in any situation not listed above, MindBridge will obtain written consent from the data subject (or their parent/guardian) before releasing personal information.

## 4.3 Disclosures in Emergencies or Legal Requirements

MindBridge reserves the right to disclose personal information **without consent** where:

- Required by law (e.g. subpoena, warrant, court order)
- Necessary to protect a student or other individual from immediate risk or harm
- Essential for public health, safety, or the enforcement of a criminal investigation
- Directed by a government body or law enforcement agency under statutory authority

All such disclosures are documented internally and reviewed by senior staff.

## 4.4 Recordkeeping of Disclosures

MindBridge maintains a secure log of all personal data disclosures, including:

- What information was shared
- To whom and why it was shared
- The legal basis or consent used
- Date and authorisation for the disclosure

This ensures **accountability, transparency, and traceability** in line with best practice in educational data protection.

# 5. Data Storage and Security

MindBridge Education takes all reasonable steps to protect the personal information it holds from misuse, interference, loss, and unauthorised access, modification, or disclosure. Security is integral to our operations, and we implement strict technical, physical, and administrative safeguards to protect the confidentiality, integrity, and availability of all personal data.

This section explains where and how data is stored, who can access it, and the systems in place to prevent breaches.

## 5.1 How We Store Personal Information





MindBridge stores personal information in both digital and physical formats:

- **Digital Records**  
Stored securely on password-protected cloud-based servers hosted in Australia or with trusted providers that comply with Australian privacy standards (e.g. Google Workspace, Microsoft 365). Sensitive documents are encrypted in transit and at rest.
- **Physical Records**  
Where paper documents are used (e.g. printed enrolment forms or signed policies), these are stored in locked cabinets at our office or school locations with restricted access.

## 5.2 Security Measures in Place

To ensure all personal data is safe from accidental or intentional threats, we implement the following security protocols:

- **Role-based access control** – Only authorised personnel (e.g. directors, program coordinators, tutors) can access personal data relevant to their duties.
- **Strong password policy** – All internal systems require secure, regularly updated passwords with two-factor authentication enabled where available.
- **Encrypted storage** – Sensitive information stored digitally is protected with industry-standard encryption.
- **Secure messaging** – Communication containing personal or sensitive data is only shared via encrypted platforms or secure portals.
- **Data minimisation** – We only collect the data necessary to deliver services and retain it for the shortest possible period.
- **Regular backups** – Our systems are backed up regularly to protect against accidental loss or system failures.
- **Paper security** – Hard-copy documents are locked when not in use and shredded when no longer required.

## 5.3 Staff Training and Obligations

All MindBridge staff and tutors undergo mandatory privacy and data protection training. They are also required to:

- Sign confidentiality and code of conduct agreements
- Understand the Australian Privacy Principles (APPs)
- Handle student and family information respectfully and legally
- Report any suspected breach or misuse immediately to the Director

## 5.4 Retention and Disposal

MindBridge retains personal information only for as long as necessary to fulfill its educational, legal, and operational obligations. Specifically:

- Student records are retained for a maximum of **three (3) years** after the student exits MindBridge's services (e.g. by graduating, withdrawing, or finishing a program).
- Tutor and employment records are retained for up to **seven (7) years**, in line with fair work and tax requirements.
- Data is securely deleted or destroyed when no longer needed. Digital records are permanently erased, and hard copies are shredded.

## 5.5 Data Breach Risk Management

MindBridge conducts regular reviews of its digital infrastructure and data handling procedures. These internal audits help:

- Identify vulnerabilities
- Ensure compliance with laws and policies
- Maintain high standards of security



In the event of an incident involving loss, misuse, or unauthorised access to personal data, MindBridge will respond immediately as outlined in **Section 6: Data Breach Notification**.

## 6. Data Breach Notification

MindBridge Education is committed to safeguarding all personal information in its care. Despite our robust security measures, we acknowledge that no system is entirely immune to risk. If a data breach occurs, we take immediate action to assess, contain, and mitigate any harm.

This section outlines how we manage data breaches and our legal obligations under the Australian Notifiable Data Breaches (NDB) scheme.

### 6.1 What Constitutes a Data Breach?

A **data breach** occurs when personal information held by MindBridge is:

- Lost (e.g. misplaced laptop, USB, or paper files)
- Accessed by an unauthorised person (e.g. hacking, internal breach)
- Disclosed to an unauthorised person (e.g. emailed to the wrong recipient)
- Modified or destroyed without authority

Not all breaches are notifiable. A breach becomes **notifiable** when it is likely to cause **serious harm** to any of the individuals whose information is involved.

### 6.2 How We Respond to a Suspected Breach

MindBridge follows a clear 4-step process when a data breach is suspected or confirmed:

**1. Contain** – We take immediate action to stop any further loss or exposure of information. This may include disabling accounts, revoking access, or securing compromised systems.

**2. Assess** – An internal investigation is conducted to determine:

- What data was affected
- How the breach occurred
- The level of risk to affected individuals

**3. Notify (If Required)** – If we determine the breach is likely to result in serious harm, we notify:

- The affected individuals
- The Office of the Australian Information Commissioner (OAIC)  
This includes details of the breach, the type of data involved, and steps individuals can take to protect themselves.

**4. Review** – After resolving the issue, we review and strengthen our processes to prevent future breaches.

### 6.3 Notification to Individuals

If the breach is deemed notifiable, MindBridge will:

- Notify affected individuals **as soon as practicable**
- Use direct communication (e.g. email or phone) where possible
- Provide a **clear, plain-English explanation** of the breach
- Recommend steps the individual should take (e.g. change passwords, monitor accounts)

If direct notification is not practical (e.g. large number of affected individuals), MindBridge may publish a notice on its website and social media channels.

### 6.4 Notification to the OAIC

MindBridge will submit a **Notifiable Data Breach Statement** to the Office of the Australian Information Commissioner (OAIC), including:

- A description of the breach
- The types of personal information involved
- Steps already taken by MindBridge
- Contact details for further inquiries
- Recommended steps for affected individuals





We will cooperate fully with the OAIC and take any additional steps required by law.

## 6.5 Preventing Future Breaches

After a breach, MindBridge reviews the incident and takes all reasonable steps to:

- Address security weaknesses
- Train or retrain staff and tutors involved
- Update internal policies or systems
- Document lessons learned and corrective actions taken

All breaches (notifiable or not) are logged internally and retained as part of our compliance records.

## 7. Access and Correction of Personal Information

MindBridge Education is committed to maintaining accurate, complete, and up-to-date records. Individuals have the right to request access to the personal information we hold about them and to request corrections where the information is inaccurate, incomplete, outdated, or misleading. This section explains how individuals can access or request corrections to their data, the process we follow, and when access may be denied.

### 7.1 Right to Access

You have the legal right to access your personal information held by MindBridge Education, including details collected during enrolment, program participation, or employment. Access requests may be made by:

- Students
- Parents/guardians (on behalf of a student under 18)
- Staff, tutors, or contractors
- Job applicants

To protect privacy, access will only be granted to the individual to whom the information relates, or an authorised legal guardian. We may require verification of identity before processing the request.

### 7.2 How to Make an Access or Correction Request

To request access to personal information, or to correct inaccurate information, individuals must:

- Submit a written request to the MindBridge Privacy Officer (see contact details in Section 9)
- Clearly identify what information they wish to access or correct
- Provide proof of identity (e.g. driver's license, school ID, Blue Card)

We aim to respond to all requests within **10 business days**.

### 7.3 Access Fees

Access to personal information is generally free of charge. However, if the request involves:

- Locating extensive archived records
- Large volumes of printed materials
- Repeated or unreasonable requests

MindBridge reserves the right to charge a **reasonable administrative fee**. We will always notify the requester of any potential costs before proceeding.

### 7.4 Correction of Information

If you believe any personal information we hold is inaccurate, incomplete, or misleading, you may request a correction. MindBridge will:

- Assess the request promptly
- Make corrections where appropriate
- Inform you in writing if we refuse the correction and provide a reason
- Allow you to add a statement to your file if the correction is not made



## 7.5 When Access May Be Denied

MindBridge may deny access in limited situations permitted by the **Privacy Act 1988**, including where:

- Granting access would pose a serious threat to the life, health, or safety of any individual
- The request unreasonably impacts the privacy of others
- The information relates to anticipated or ongoing legal proceedings
- Access would prejudice negotiations, investigations, or enforcement activities
- The request is deemed frivolous or vexatious

In such cases, we will provide written notice with the reasons for refusal and information on how to make a complaint (see Section 9).

## 8. Consent and Rights of Access for Parents and Students

MindBridge Education recognises the sensitive nature of working with minors and the legal responsibility to balance the rights of students with the authority of parents or guardians. This section outlines how we manage parental consent, student access to their own information, and situations where independence or confidentiality may apply.

### 8.1 Parental Consent

MindBridge relies on parents or legal guardians to provide consent on behalf of students under 18 years of age when:

- Enrolling in a tutoring program
- Authorising the collection or disclosure of sensitive personal information
- Agreeing to photo, video, or testimonial use for marketing
- Providing emergency medical instructions
- Accepting the Privacy Policy and Terms of Use

Where both parents share legal responsibility, we generally require consent from one parent only unless otherwise requested by law, court order, or in cases of parental dispute.

Consent granted by a parent is treated as valid consent on behalf of the student.

### 8.2 Student Rights and Independent Access

MindBridge recognises that students mature at different rates, and the level of privacy afforded may depend on the student's **age, maturity, capacity to understand**, and the **context** of the request.

We may allow a student to:

- View or correct their own personal information
- Provide consent for use or disclosure
- Participate independently in decision-making related to their program

Such decisions are made at the discretion of MindBridge staff based on:

- The student's ability to understand the nature and consequences of the request
- Whether granting access is in the student's best interests
- Any risks posed by withholding information from a parent

In general, students aged 15 and over are presumed capable of making independent decisions regarding their personal data, unless evidence suggests otherwise.

### 8.3 Withholding Information from Parents

In rare cases, MindBridge may decline to provide parents with access to their child's personal information if:

- It would **unreasonably impact the privacy or safety** of the student
- The student has explicitly requested that certain information remain confidential
- A duty of care, legal restriction, or safeguarding concern applies



All such decisions will be carefully documented, assessed by senior management, and made with the student's best interests and legal rights in mind.

## 8.4 Changes to Consent

Parents and students may withdraw or change consent at any time by:

- Submitting a written request via email
- Confirming identity
- Clearly stating what consent is being modified or withdrawn

MindBridge will confirm receipt and update its records accordingly within a reasonable timeframe.

## 9. Enquiries and Complaints

MindBridge Education is committed to protecting the privacy of all individuals who engage with our services. We welcome feedback and take all enquiries and complaints regarding personal information seriously. Our goal is to resolve any privacy-related concerns in a respectful, lawful, and timely manner.

### 9.1 General Enquiries

For general questions about this Privacy Policy, how your personal information is handled, or how to access or correct your data, individuals are encouraged to contact our Privacy Officer.

All enquiries will be treated confidentially and handled by trained staff authorised to assess and respond appropriately.

### 9.2 How to Lodge a Privacy Complaint

If you believe that MindBridge Education has breached your privacy or mishandled your personal information, you may submit a formal complaint. To do so:

- Submit a written complaint (email or letter) to the contact below
- Include your full name and contact details
- Clearly describe the issue, including relevant dates, names (if known), and supporting documentation
- State the outcome you are seeking

Complaints should be addressed to:

#### Privacy Officer

MindBridge Education Pty Ltd  
info@mindbridgeedu.com.au  
0414082007  
Brisbane QLD

### 9.3 Our Response Process

Upon receiving your complaint, MindBridge will:

- Confirm receipt of the complaint within **3 business days**
- Investigate the matter thoroughly, including speaking with relevant staff
- Contact you if further details are needed
- Aim to provide a full written response within **10 working days**

If more time is required (e.g. due to complexity), we will inform you of the delay and expected timeframe.

We will strive to resolve your complaint fairly and transparently, in accordance with the **Australian Privacy Principles**.

### 9.4 Escalation to the OAIC

If you are dissatisfied with MindBridge's response, or feel your concerns have not been adequately addressed, you may refer your complaint to the **Office of the Australian Information Commissioner (OAIC)**. The OAIC is the independent regulator for privacy matters in Australia.

**Contact details:**

Office of the Australian Information Commissioner (OAIC)

GPO Box 5218, Sydney NSW 2001

Phone: 1300 363 992

Email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

Website: [www.oaic.gov.au](http://www.oaic.gov.au)

MindBridge will fully cooperate with the OAIC during any external review or investigation.

**10. Using Other Websites**

MindBridge Education's website and communication channels may include links, references, or integrations with third-party websites, platforms, and tools. These may include scheduling platforms, learning portals, secure payment gateways, social media profiles, or external educational resources.

While we aim to partner only with reputable providers, MindBridge is **not responsible** for the content, privacy practices, or data security measures of third-party websites.

**10.1 No Control Over External Content**

Once you leave our website or platform—by clicking a link or accessing an embedded tool—you are no longer covered by this Privacy Policy. We cannot guarantee the privacy standards, terms of use, or security controls of any third-party service.

Examples of external services may include:

- Online forms hosted by Google Forms or Typeform
- Scheduling tools (e.g. Calendly or BookedIn)
- Educational platforms (e.g. Edmodo, ClassDojo, or Canvas)
- Payment gateways (e.g. Stripe, PayPal)
- Partner school websites
- Social media platforms (e.g. Instagram, Facebook, LinkedIn)

We strongly recommend that you read the privacy policies and terms of service of any third-party site before submitting personal information.

**10.2 Embedded or Integrated Tools**

If MindBridge integrates third-party systems (such as embedded videos, chat boxes, analytics, or booking widgets) into our website or online services, these tools may also collect user data. Where applicable, we will:

- Clearly notify users when third-party tools are in use
- Minimise unnecessary data collection through those tools
- Ensure that third-party providers follow reasonable privacy practices

However, we cannot be held liable for how these external tools collect, store, or use your information once it is submitted through their system.

**10.3 User Responsibility**

It is your responsibility to use discretion when interacting with any external links or content. If you have questions or concerns about any third-party website or tool featured through MindBridge Education, we encourage you to contact them directly.

**11. Policy Management**

MindBridge Education is committed to keeping its Privacy Policy accurate, up-to-date, and compliant with all relevant legal and operational requirements. As privacy laws, technologies, and our services evolve, we may review and amend this policy periodically to reflect those changes. This section outlines how we manage updates and communicate those changes to affected individuals.

**11.1 Review and Update Cycle**



We review this Privacy Policy:

- At least **once every 12 months** as part of our annual compliance process
- **Immediately following any changes** to the Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), or data protection obligations affecting the education sector
- **After any major change** in our service delivery model, such as the introduction of new platforms, systems, or partnerships that affect how we collect or use personal data

Any updates are reviewed and approved by senior management or the appointed Privacy Officer to ensure compliance and clarity.

## 11.2 Notification of Changes

When material changes are made to this Privacy Policy, MindBridge might

:

- Publish the updated policy on our official website ([www.mindbridgeedu.com.au](http://www.mindbridgeedu.com.au))
- Include a "Last Updated" date at the top of the policy
- Notify affected individuals (e.g., students, parents, tutors, partner schools) via email, in-app notification, or during program onboarding
- Provide access to archived versions of previous policies on request

By continuing to use our services after any changes are made, you are deemed to have accepted the updated Privacy Policy unless you notify us otherwise.

## 11.3 Archived and Previous Versions

MindBridge maintains digital records of all past versions of this Privacy Policy. Individuals may request copies of prior versions to understand what terms applied at the time of their data collection or service use.

## 12. Annexure A – Standard Information Collection Notice

This Standard Information Collection Notice explains how and why MindBridge Education collects personal information from students, parents, tutors, and other individuals. It should be made available at the time personal data is collected — such as during program enrolment, form submissions, onboarding, or employment applications.

### 12.1 Student and Parent Collection Notice

MindBridge Education Pty Ltd ("MindBridge") collects personal information, including sensitive information, about students and their parents or guardians before and during the course of enrolment in any MindBridge program.

We may collect this information via online forms, paper applications, interviews, emails, phone calls, and in-person discussions with staff. Occasionally, information may also be obtained from third parties such as schools or health professionals.

The primary purpose of collecting this information is to enable MindBridge to:

- Deliver structured academic support tailored to student needs
- Communicate with parents/guardians and partner schools
- Monitor student progress, attendance, and wellbeing
- Support health, safety, and duty of care requirements
- Meet contractual, legal, and administrative obligations

We may also use this information for program evaluation, de-identified reporting, or future marketing and communications (only with consent).

If the requested information is not provided, we may be unable to enrol the student or provide the full range of services safely and effectively.

MindBridge may disclose personal information to:



- Tutors or staff directly involved in supporting the student
- Partner schools for reporting and alignment purposes
- Medical professionals (in emergencies)
- Government or regulatory authorities (as legally required)
- Technology service providers (e.g., learning platforms, email tools)
- Third parties authorised by you or required by law

Personal information may be stored in cloud-based systems, which could involve servers located outside Australia. We ensure all third-party service providers are contractually bound to uphold privacy standards equal to or exceeding Australian law.

For more information, including how to access or correct your information or to lodge a privacy complaint, please refer to our full Privacy Policy at [insert website] or contact:

### Privacy Officer

MindBridge Education Pty Ltd

Email: [info@mindbridgeedu.com.au](mailto:info@mindbridgeedu.com.au)

Phone: 0414082007

## 12.2 Staff and Tutor Application Collection Notice

When applying for employment or contract work with MindBridge, you will be required to provide personal information. We may also collect personal information from referees, previous employers, or public sources relevant to your qualifications.

This includes (but is not limited to):

- Name, contact information, and work history
- Academic transcripts and certifications
- Blue Card or Working with Children Check details
- Bank and superannuation information (if hired)
- Health or criminal record details (only where relevant and with consent)

If your application is unsuccessful, we may retain your details for up to 12 months for consideration in future roles unless you request otherwise.

MindBridge will not disclose your personal information outside the recruitment process except where required by law or contract (e.g., for Blue Card screening or insurance compliance).

For more on how we handle staff and applicant data, please refer to our full Privacy Policy or contact our Privacy Officer.

## 13. Optional Addendum A – Photography and Media Consent

MindBridge Education may occasionally take photos or videos during tutoring sessions, workshops, or school visits for promotional or educational purposes. Any such images that include students will only be used with:

- **Written consent** from a parent or guardian (for students under 18), or
- **Direct consent** from the student if they are over 18 and capable of providing informed permission

Consent forms will clearly specify:

- The purpose (e.g., social media, website, brochure)
- Whether names or identifying features will be included
- How long the content may be used or stored

No media will ever be used for marketing without explicit, signed consent. Individuals may withdraw consent at any time by contacting our Privacy Officer.

## 14. Optional Addendum B – Cookie and Website Tracking Policy



MindBridge Education's website may use cookies and other tracking technologies to enhance user experience and monitor site performance.

Cookies are small text files stored on your device when you visit a website. We may use them to:

- Remember your preferences
- Improve website speed and layout
- Track traffic sources, page views, and device types via analytics tools (e.g., Google Analytics)
- Secure login or booking forms

Users can disable cookies in their browser settings at any time. Our use of cookies does **not** collect sensitive information, nor do we use cookies for behavioural advertising or profiling.

## 15. Optional Addendum C – Data Retention and Deletion Policy

MindBridge Education retains personal information only for as long as necessary to fulfil its purposes, including legal, reporting, or administrative requirements. Once no longer needed, personal information is securely deleted or destroyed.

- Student data: retained for up to 3 years after program completion or withdrawal
- Tutor/employee data: retained for up to 7 years (e.g., for tax and payroll compliance)
- Applicant data: retained for up to 12 months unless requested otherwise
- Marketing opt-in data: removed within 5 business days upon request
- Digital backups: destroyed in regular, scheduled deletion cycles

Requests for early deletion of personal information must be made in writing and will be assessed in accordance with applicable law and policy.

## 16. Final Statement and Contact Summary

MindBridge Education takes its privacy responsibilities seriously and is committed to maintaining a high standard of transparency, accountability, and legal compliance in all matters related to personal information.

This Privacy Policy reflects our core values of trust, safety, and educational integrity. It is designed to:

- Protect the rights of students, parents, staff, and schools
- Provide clarity about how data is collected, stored, used, and shared
- Fulfil all obligations under the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles**

By engaging with MindBridge Education, you acknowledge and accept the terms outlined in this Privacy Policy.

We encourage all individuals to review this document regularly and reach out with any questions or concerns. Open communication is essential to building lasting trust between our organisation and the communities we serve.

## Contact Details for All Privacy Matters

### Privacy Officer

MindBridge Education Pty Ltd

Brisbane, QLD

Email: [info@mindbridgeedu.com.au](mailto:info@mindbridgeedu.com.au)

Phone: 0414082007

Website: [www.mindbridgeedu.com.au](http://www.mindbridgeedu.com.au)