# Privacy & Security Pack

Supplier inputs for a school Privacy Impact Assessment

Written for the person completing a school Privacy Impact Assessment. The school remains responsible for its own PIA; this supplies the vendor inputs those templates ask for, so they can be attached rather than requested.

| | |
|---|---|
| SUPPLIER | **DiscoverWorthy · ABN 74 694 878 594** |
| REGISTERED ADDRESS | **140 Keilor Road, ESSENDON NORTH, VIC 3041** |
| GOVERNING LAW | **Australia** |
| DATA REGION | **Microsoft Azure · Australia East** |
| PRIVACY CONTACT | **dpo@discoverworthy.com** |
| SECURITY & INCIDENTS | **security@discoverworthy.com** |

## 1. What the product is

### What does the school use it for?

A managed website and content platform: the school's public site, its notices, calendar and published articles, plus staff logins to maintain them. Optionally, a member register for the school community.

### Does it collect student data?

Not by default, and it is not required. A school can run entirely on staff and business information.

The member register *can* hold records for students if the school chooses to use it, including a junior indicator, documents attached to a named person, and guardian access. Nothing enables this automatically and nothing populates it without the school entering the data. If you intend to use it that way, assess sections 4 and 5.

## 2. Where data is held

### In which country and region is data stored?

Australia. Production database, file storage, application servers and the AI service that processes member content all run in Microsoft Azure, Australia East (Sydney).

### Does any data leave Australia?

Yes, in one defined case, stated here so it is not discovered later. Generating website copy and illustrations uses services hosted in the United States (see section 3). These receive the business information the school publishes about itself. They do not receive member records, member documents, or member portal activity.

## 3. Sub-processors

| PROVIDER | PURPOSE | LOCATION |
|---|---|---|
| **Microsoft Azure** | Hosting, database, file storage, AI processing of member content | Australia East (Sydney) |
| **Cloudflare** | Delivery and caching of the published public website | Global edge network |
| **Stripe** | Payment processing, where the school pays by card | United States / global |
| **Anthropic** | Generating website copy from information the school publishes | United States |
| **Google (Gemini)** | Generating illustrations and cover images | United States |
| **Twilio** | SMS notifications, where enabled | United States / global |

| | | |
|---|---|---|
| **Azure Communication Services** | Transactional email (notifications, sign-in codes) | Microsoft Azure |
| **Brave Search** | Search data used for content research | United States |

Not every provider is engaged for every school — SMS and payments apply only where used.

## 4. Security controls

**Is data encrypted?**

At rest: the database uses Azure SQL Transparent Data Encryption, and file storage is encrypted by the platform. In transit: HTTPS throughout, with a TLS 1.2 minimum.

**How is access controlled?**

Staff access is per-account with role-based permissions. Member portal access is separate and gives a person sight of their own records only.

Documents attached to a person are not public links. Each request is authorised against the person asking, and a request for something you are not entitled to returns nothing rather than an error confirming it exists. Downloads are recorded.

**Who can see a student's documents?**

The student, and any adult the school has explicitly authorised. A parent cannot grant themselves access, and a guardian cannot grant it to someone else. The record retains who granted access and when; withdrawal is recorded rather than erased, so the school can answer who had access between which dates.

**Is consent recorded for student stories?**

Where a school publishes a student profile, consent for a junior goes to their guardian and is bound to that exact version of the text. Editing the story afterwards invalidates the previous approval, so consent cannot be obtained on one draft and spent on another.

**Is the service monitored?**

Yes — continuous automated health checks across the application, database and dependencies, alerting on failure rather than relying on someone noticing.

**What are your backup and recovery arrangements?**

Backups are Azure's managed database backups with point-in-time restore. We confirm the current retention window and recovery objectives in writing against your template rather than publish figures your assessment would then need to verify.

## 5. Collection, retention and deletion

**What is collected?**

School and staff details needed to operate the account (names, work contact details, sign-in records), the content the school creates, and — only if the school uses the member register — the member details it enters, which may include documents.

**How long is it kept?**

For as long as the account is active, and for as long as the school asks us to keep it. We do not impose a retention period on your content.

**Can we get our data deleted?**

Yes. On request we delete the records and the files behind them. That distinction is deliberate: a document about a named child is destroyed, not merely unlinked from the record describing it.

**Can we export our data?**

Yes — your content is yours, and we export it on request.

**Is data sold or used for advertising?**

No. We do not sell data, do not share it with advertisers, and do not use it to train third-party models.

## 6. Compliance and incidents

**Do your staff need a Working with Children Check?**

We are a software supplier and do not attend school sites or work directly with students, so a WWCC is not applicable to the service. If an engagement ever changed that, we would raise it beforehand.

**What happens in a data breach?**

We notify the school promptly with what we know, what was affected and the steps taken, so the school can meet its own obligations under the Notifiable Data Breaches scheme and the requirements of its jurisdiction. This is a documented plan, published as our AU Notifiable Data Breach Plan.

## 7. Anything not answered here

If your template asks something this pack does not cover, ask us directly and we will answer it in writing — dpo@discoverworthy.com. We would rather answer a specific question than have an assessment stall on a gap.