Privacy Policy

DigiMe Educational Consulting · ABN 35 834 126 324 · Version 1.5 · Effective 21 November 2026

PulsePoint is a check-in/check-out tool that schools use to run their PBIS (Positive Behaviour Interventions and Supports) program. This policy explains what information PulsePoint holds, why, where it is kept and how it is looked after. It is written for the school leaders who sign up, the staff who use it every day, and the parents who receive reports from it.

1. Who we are

PulsePoint is made and operated by DigiMe Educational Consulting (ABN 35 834 126 324), based in Adelaide, South Australia. In this policy "we", "us" and "our" mean DigiMe Educational Consulting. We comply with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

This policy covers the PulsePoint app at pulsepoint.digimeec.com.au and the emails it sends. Our website at digimeec.com.au and our consulting work have their own privacy policy.

2. Your school is in charge of its data

Everything in PulsePoint is entered by your school: its staff add students, score days, write notes and enter parent email addresses. Your school decides what goes in, who at the school can see it, and when it is removed. Under the Privacy Act your school is the organisation responsible for that information, and we hold and process it on the school's instructions.

We only use school data to provide PulsePoint to that school. We do not sell it, share it with advertisers, use it to train AI systems, or combine it with data from other schools. Our own staff look at a school's data only to provide support the school has asked for, to investigate a fault or security concern, to bill the school, or where the law requires it.

3. What PulsePoint holds

About students (entered by school staff): name, year level, which teachers and mentor they are assigned to, the goal and dates of their program, daily behaviour ratings (0 to 3 for each expectation in each session), check-in and check-out moods, mentor notes, celebration badges, and any notes staff add. Nothing is collected from students themselves; students never sign in.

The school's student list: a school administrator can upload the school's student list, or add students to it one at a time. For each student it holds the Student ID, first and last name, year level, roll class and up to two parent/carer email addresses, so a program can be started without retyping those details. The uploaded file itself is not kept. Its contents are held only while an administrator reviews them. An upload that is not confirmed within 24 hours can no longer be confirmed, and is deleted at the next daily clean-up, within two days. The file's name and the email of the administrator who uploaded it are kept as a record of each upload. The student list is stored with the rest of the school's data, in Australia, and is visible only to school administrators. A student who leaves stays on the list, marked as left.

Student photos: a school administrator can add a photo for each student on the student list, usually the school's own portrait photo, named by Student ID. Each photo is made small in the browser before it is sent, then stored as a 256 by 256 pixel picture; this removes any information the camera added, such as location. The original file is not kept. Photos are stored encrypted, with the key that protects them held by Microsoft Azure Key Vault in Australia (see section 8). A photo is shown to the school's staff who can see that student, beside the student's name, and on the parent's daily report page. Photos are never put in an email, the CSV export or the PDF report. Because photos are sensitive, a student's photo is deleted as soon as they are marked as having left the school. All their other records are kept as before.

About parents and carers: the email addresses the school enters for each student, and a record of when a daily report was emailed to them and when the link was opened.

About school staff: name, email address, role (teacher or leadership mentor), whether they are a school administrator, and how they sign in. For password sign-in we store a one-way hash of the password, never the password itself. For Microsoft sign-in we store the Microsoft account identifier and tenant that authorised them.

About the school: school name, the contact name and email given at sign-up, the plan and its expiry date, the school's logo if one is uploaded, and the identifiers Stripe gives us for the school's customer, subscription, payments and invoices. We never see or store card numbers.

Technical records: an audit log of changes (who did what, when, from which IP address), sign-in attempts (email address and IP address, used to slow down password guessing), and a session record while someone is signed in.

4. Why we hold it

- To run the program: showing each day's form, calculating scores, producing progress reports and PDFs, and archiving students when a program ends.

- To help staff, and parents on the daily report page, see at a glance which student a record is about, when the school adds student photos.
- To send the emails the school asks for: a daily report to a student's parents, a notice to a teacher or mentor when a student is assigned to them, a reminder of the specialist sessions a staff member has today, and account emails such as invitations and password resets.
- To keep accounts secure: checking sign-ins, limiting repeated failures, signing people out after 30 minutes of inactivity, and keeping an audit trail a school can ask us about.
- To bill the school and keep the business records the law requires.
- To support the school when it contacts us.

We do not use the information for any other purpose, and we do not send marketing email from PulsePoint.

5. Children's information

PulsePoint holds information about children's behaviour at school, which their school treats with care and so do we. The school collects it under its own policies and its duty of care, decides which staff can see it, and is the right place for a parent to go with questions about what has been recorded. Teachers can only see the students assigned to them; leaders and mentors can see the whole school.

We never contact students, parents or teachers via any address the school has entered for that child. A parent's report link shows one day's summary for one child and stops working 24 hours after it is sent.

6. Where it is stored

All PulsePoint data is stored in Australia on servers operated for us by AITS, and it is not transferred overseas. Backups are kept in Australia too. Both Stripe and Microsoft are operated overseas and receive only limited essential information, as required by them to operate, described in the next section: Stripe, for payments, and Microsoft, for Single Sign-On and for the key that protects student photos. That key is held by Microsoft Azure Key Vault in Australia; the photos themselves stay on our servers in Australia.

7. Who else is involved

We do not share school data with anyone except the providers below, each of which acts for us and receives only what is listed. We disclose information where Australian law requires it and tell any school unless the law prevents that.

Who	What they do for us	What they receive
AITS (Australia)	Hosts the PulsePoint servers, database and backups	Everything PulsePoint stores. Located in Australia.
Stripe (Stripe Payments Australia Pty Ltd, part of a US company)	Takes card payments and issues invoices	School name, contact name and email, plan and amount. Card details are entered on Stripe's own page and never reach PulsePoint. For schools that pay by card, Stripe keeps the card on file to renew the subscription each year; PulsePoint stores only Stripe's customer and subscription references, never card details.
Microsoft (Entra ID and Azure Key Vault)	Optional "Sign in with Microsoft" for schools that turn it on; Azure Key Vault holds the key that protects student photos, in Microsoft's Australia East region	The sign-in happens with Microsoft. PulsePoint receives the staff member's name, email address, tenant ID and Microsoft account ID. For photos, Key Vault receives only a school's photo key, to lock or unlock it — no photo, name or other student data is sent to Microsoft.

Email is sent from our own server, from noreply@digimeec.com.au, and not through a third-party mailing service.

8. How it is protected

- All connections to PulsePoint are encrypted (HTTPS). The site refuses unencrypted connections.
- Databases are secured from any public-facing web traffic.
- Passwords are stored as one-way hashes. Schools can alternatively use Microsoft SSO instead for added site security.
- Student photos are encrypted, each school's with its own key, and that key can be unlocked only by Microsoft Azure Key Vault in Australia.
- Access is by role: teachers see only their assigned students. All requests check the signed-in user's school and role before touching any record.
- Repeated failed sign-ins lock the account temporarily and public forms are rate-limited.
- Every change action to a record is written to an audit log.
- The database is backed up daily, each backup is integrity-checked, and backups are kept within Australia.
- Card details are entered on Stripe's payment page, never on ours. For schools that pay by card, Stripe keeps the card on file to renew the subscription each year; PulsePoint stores only

Stripe's customer and subscription references, never card details. Stripe use is in accordance with their Terms of Service.

Student photos are the one part of the stored data that is encrypted at rest. Each school's photos are encrypted with that school's own key, which is kept only in a locked form that Microsoft Azure Key Vault must unlock each time photos are shown or saved. A stolen copy of the database or of a backup therefore shows no photos; Microsoft keeps a record of every use of the key; and we can cut off access to it in Azure. It does not protect against someone who has taken full control of our server, who could still ask Key Vault to unlock keys. The rest of the stored data is not encrypted at rest; it is protected by the server's access controls and the private location described above. No online service can promise perfect security, and we ask schools to keep their staff accounts to the people who need them and to remove staff who leave.

9. How long we keep it

What	How long	Notes
Student records, daily scores, notes and archived students	For as long as your school has an active subscription or trial, then 90 days	Renew within 90 days of expiry and everything is as you left it. Ask for an export at any time before deletion.
School student list (Student ID, name, year level, roll class, parent/carer email addresses)	Until your school deletes a student from the list, or the school's data is deleted	Your school decides what to upload. A student who leaves stays on the list, marked as left, so their past records can still be found.
Student photos	Until the student is marked as having left the school, is deleted from the student list, or the school's data is deleted	Because photos are sensitive, a student's photo is deleted as soon as they are marked as having left the school. All their other records are kept as before.
Parent report links	The link stops working 24 hours after it is sent; the record of the send is deleted after 90 days	The daily record it pointed to stays with the student.
Staff accounts	Until your school removes the person, or the school's data is deleted	A removed staff member can no longer sign in; their name stays on historical records they created.
Audit log (who changed what, and from which IP address)	2 years	Kept so a school can answer questions about a record's history.

What	How long	Notes
Sign-in attempts and rate-limit counters (IP address, email address)	30 days	Used only to slow down password guessing.
Password reset, welcome and invite links	Between 1 hour and 7 days, depending on the link	Expired links are useless; the rows behind them are deleted with the rest of the school's data.
Payment records (date, amount, payment method, payment reference and any note, filed under the school's account username, which can be an email address)	7 years after the payment date, then deleted	Australian tax law requires us to keep business records for this long, so these are kept even after the rest of a school's data is deleted. No card numbers are held.
Backups	30 daily copies and 12 monthly copies	A record deleted from the live database can remain in a backup for up to 12 months, then it is gone.

A school leader can archive or delete a student, and remove a staff member, from inside PulsePoint at any time. A school can ask us to delete all of its data at any time by emailing info@digimeec.com.au; we do so within 30 days and confirm in writing. Payment records are the one exception: we keep them for the period in the table above, even after the rest of a school's data is deleted.

10. Access and correction

A school leader can view, edit and export the school's own data from inside PulsePoint. Staff and parents who want to see or edit information about themselves or their child should contact the school first. If you would rather contact us, email info@digimeec.com.au; we will respond within 3 days, and we will involve your school where the request is about its data.

11. If something goes wrong

If we become aware of a data breach involving a school's data, we will inform each school as soon as practicable and no later than 72 hours after we become aware of it. We will inform what we know, who is involved and who has been notified. We will help the school meet its own obligations under the Notifiable Data Breaches scheme, and we will notify the Office of the Australian Information Commissioner (OAIC) ourselves where the scheme requires us to.

12. Cookies

PulsePoint uses one cookie, to keep you signed in. It is deleted when you sign out or after 30 minutes of inactivity. There are no advertising or analytics cookies.

13. Complaints

If you think we have not handled personal information properly, please contact us first using the details below. We will acknowledge your complaint within a week and aim to resolve it within 30 days.

14. Changes to this policy

When we change this policy we update the version and effective date at the top. If a change affects what we hold or how we use it, we will email each school's administrators before it takes effect. The current version is always at pulsepoint.digimeec.com.au/privacy.php.

15. Contact

Matt Richards, DigiMe Educational Consulting

ABN 35 834 126 324

Email: info@digimeec.com.au

Phone: 0403 911 814

Adelaide, South Australia
