

# Privacy Policy

Your Timesheet — operated by emedu

Effective: [DATE OF PUBLICATION] ABN: [ABN] Privacy contact: [privacy@yourtimesheet.com.au]

The three placeholders above are facts only emedu can supply. Everything else is complete and describes the service as built.

---

## 1. About this policy

This policy explains what personal information Your Timesheet collects, why, who it goes to, and what you can do about it. It is written to comply with the Australian Privacy Principles in the *Privacy Act 1988* (Cth).

We comply with the Australian Privacy Principles whether or not the Act currently obliges us to. A small business may fall outside the Act on turnover, and that exemption is under active reform. Rather than rely on an exemption that may not apply and may not last, we hold ourselves to the Principles now.

Where we handle information on behalf of an employer that has its own privacy obligations — a public sector body, for example — we expect to be bound by those obligations through our contract with them. For a Victorian public sector employer that means the *Privacy and Data Protection Act 2014* (Vic).

## 2. What Your Timesheet does, and what it is not

Your Timesheet automates the filling in of a timesheet. You upload your roster, the system fills a timesheet in, it comes back to you to check on the day it is due, and you send it to your employer. That is the whole of the service.

It is worth being explicit about what it is not, because it shapes what we hold and for how long:

- **It is not a record-keeping service.** We are not where your employment records live. Your employer holds those, and is obliged to. We produce a document, send it, and let go of it.
- **It is not a payroll system.** We do not calculate pay, apply award or agreement rates, or determine what you are owed. We add up hours you entered. What those hours are worth is between you and your employer.
- **It is not a compliance service.** We do not assess or advise on award, enterprise agreement or Fair Work obligations, and nothing the service produces should be treated as advice about your entitlements.
- **It is not a tax service.** We have nothing to do with the Australian Taxation Office and hold no tax information.

Because we are none of those things, we keep as little as possible, for as short a time as we can.

## 3. Anonymity and pseudonymity

You cannot use Your Timesheet anonymously. A timesheet is a claim for payment made by a named person to a named employer, and an email address is how we establish that the person sending it is the person it belongs to. This is a limitation we consider necessary, and it is the reason we collect as little else as we can.

## 4. What we collect

**Your account.** Your email address, and a password. We do not store the password. We store a one-way Argon2id hash of it, which cannot be reversed — this is why we can reset a password but never tell you what it was.

**Your details.** Your name, employee or personnel number, classification and employment status, if you enter them. These are optional. The service works with them blank and you can write them on the printed form instead.

**Your roster, if you choose to keep one.** Only your own shifts. A ward or unit roster names other people; the file is filtered in your browser and only your rows are sent to us. Your colleagues' shifts never reach our systems.

**Your workplace's rules.** Your organisation's name, department, standard shift times, pay-cycle dates and submission deadline. These are set by an administrator at your organisation and apply to everyone in it.

**A record of each timesheet sent.** The pay period, the address it went to, the total hours, the file size, and a cryptographic fingerprint of the file. Enough to establish that you sent what you say you sent, and when.

**Technical information.** Your IP address and browser identification on sign-in attempts, used to detect and slow attacks on accounts.

## 5. What we do not collect

- **We do not collect health information**, and we ask you not to enter any. A timesheet records hours worked. The comments field is for notes about the shift — a late finish, a call-out — not for anything about your health or, if you work in healthcare, anyone else's.
- **We do not collect government identifiers.** No tax file number, no Medicare number, no licence or passport details. An employee number is your employer's identifier, not a government one.
- **We do not collect payment card details.** Where a paid plan applies, payment is arranged separately and card details do not pass through this service.
- **We do not keep sent timesheets.** The spreadsheet is generated, emailed and discarded.
- **We never receive your signature.** If you sign a sheet on screen, the signature is placed onto the file inside your own browser and is never uploaded.
- **We do not track you.** No advertising trackers, no analytics services, and no third-party scripts beyond the fonts and libraries needed to display the page.
- **We do not use your information to train artificial intelligence.**

## 6. Why we collect it, and what happens if you don't provide it

We collect this information to create and secure your account, produce your timesheet, apply your workplace's rules to it, send it where you tell us, keep a record that you sent it, and protect accounts from unauthorised access.

If you decline to provide your name and employee number, we can still produce a timesheet; you will need to write those details on it yourself. If you decline to provide an email address, we cannot provide the service at all.

## 7. Who we disclose it to

**Your employer**, at the address you enter — normally your payroll team, or whoever approves timesheets where you work. This is the purpose of the service.

**Yourself**. Every timesheet is copied to the address you registered with, so you keep your own record of what you submitted.

**Administrators at your organisation**, who can see the email addresses and roles of members and the workplace rules they have set. They cannot see the contents of your timesheets, because we do not retain them.

**Amazon Web Services**, which hosts the application, the database, the encryption keys and the email delivery service.

We do not sell personal information. We do not disclose it for direct marketing. We do not disclose it to anyone else except where required or authorised by Australian law, or where necessary to protect someone's safety.

## 8. Overseas disclosure

All data is stored and processed in Amazon Web Services' Sydney region (ap-southeast-2) and is not transferred overseas in the ordinary operation of this service.

Amazon's global support and engineering functions may in limited circumstances access infrastructure from outside Australia, under AWS's own contractual and security controls. We make no other disclosure of personal information to overseas recipients.

## 9. Direct marketing

We do not use your personal information for direct marketing. The only emails we send are the ones the service requires: confirming your address, resetting your password, your timesheet to check, a reminder when your roster is running out, and the timesheet itself.

## 10. How we protect it

- Connections use TLS. Session cookies cannot be read by scripts.
- Passwords are hashed with Argon2id and cannot be recovered, only reset.
- Your details, your roster and your workplace's rules are encrypted before storage using AES-256-GCM, under keys held in AWS Key Management Service. A stolen copy of the database cannot be read without those keys.
- Session identifiers are stored as one-way hashes, so a copy of the database cannot be used to impersonate you.
- Sign-in attempts are rate-limited, and accounts lock temporarily after repeated failures.
- Changing your password ends every session on every device.
- Access to production systems is limited to those who need it.

No system is perfectly secure. The strongest protection here is that we hold very little: a timesheet you have sent exists in your inbox and your employer's, not on our systems.

## 11. Automated processing

The service calculates hours from the times you enter, including shifts that run past midnight, and fills a timesheet in from a roster you upload. These are arithmetic and formatting steps.

**No decision about you is made automatically.** Nothing goes to your employer until you have seen it and pressed send. The calculated hours are a starting point you are expected to check and correct, and the figures your employer receives are the ones you approved.

## 12. How long we keep it

| What                                    | How long                                          |
|-----------------------------------------|---------------------------------------------------|
| Account and organisation records        | Until the account is deleted                      |
| Your details and your workplace's rules | Until changed, or the account is deleted          |
| A kept roster                           | Until 30 days after the cycle it covers has ended |
| A timesheet awaiting your confirmation  | Until you send it, or 14 days                     |
| The record that a timesheet was sent    | 12 months                                         |
| Sign-in attempt logs                    | 90 days                                           |
| Expired sessions and used links         | Removed automatically                             |
| Sent timesheets                         | Not kept at all                                   |

The record of a send holds no hours detail — only that a timesheet was sent, when, to whom, a fingerprint of the file, and that you confirmed the hours were correct before it went. We keep it for twelve months so that a recent query can be answered, and then delete it. We are not the keeper of your employment records: those are your employer's, and your own copy of every timesheet is in your inbox.

## 13. Accessing and correcting your information

You can see and change your details, your kept roster, and your workplace's rules if you are an administrator, inside the service at any time.

To request a copy of everything we hold about you, to ask for a correction, or to ask us to delete your account and its data, contact us at the address at the top of this policy. We will respond within 30 days, and there is no charge.

If we refuse a request we will tell you why in writing, and how to complain.

Timesheets already emailed to your employer are your employer's records. We cannot recall them, and deleting your account does not remove them from your employer's systems.

## 14. Data breaches

If a data breach occurs that is likely to result in serious harm, we will assess it promptly and notify affected individuals and the Office of the Australian Information Commissioner, in accordance with the Notifiable Data Breaches scheme. Where the information concerns a health service's staff, we will also notify that organisation without delay so it can meet its own obligations.

## **15. Cookies**

One cookie is set: a session identifier that keeps you signed in. It is essential to the service, expires after 12 hours, and is not used for tracking. We set no advertising or analytics cookies.

## **16. Children**

The service is intended for people in paid employment. It is not directed at children and we do not knowingly collect information from them.

## **17. Complaints**

If you are concerned about how we have handled your personal information, please contact us first at the address at the top of this policy. We will acknowledge your complaint within 5 business days and respond within 30 days.

If you are not satisfied with our response, you can complain to the Office of the Australian Information Commissioner:

- [oaic.gov.au](http://oaic.gov.au)
- 1300 363 992
- GPO Box 5218, Sydney NSW 2001

## **18. Changes to this policy**

We will publish any material change here and notify you inside the service before it takes effect.