PRIVACY POLICY

Cybermate Privacy Policy

What Cybermate collects about people, why, who sees it, and the choices and rights you have

Version 2026-11-04

Written for: Everyone whose information Cybermate handles: people who use Cybermate through their organisation, administrators, people who sign up, and visitors to our website.

Document details

Item	Detail
Document	Cybermate Privacy Policy
Version	2026-11-04 (effective 4 November 2026)
Who we are	Sycurus Australia Pty Ltd, ABN 19 649 664 013, ACN 649 664 013, trading as Cybermate
Registered address	11/14-28 Blues Point Road, Mcmahons Point NSW 2060
Privacy questions, access requests and complaints	support@cybermate.com.au

About this document

Cybermate helps organisations teach their people to spot scams and use AI safely. To do that we handle personal information. This policy explains what we collect, why, who can see it, who else handles it, how long we keep it, and how you can see it, correct it, have it removed or complain.

It follows the Privacy Act 1988 (Cth) and the Australian Privacy Principles. Where we say what the platform does, that is how it works at the date of this policy. We say so plainly where it does not yet do something you might expect.

Contents

01	1. Who we are, and our two roles	4
02	2. What we collect	4
03	3. How we collect it	6
04	4. What we use it for	7
05	5. Who can see your information inside your organisation	7
06	6. Who else handles your information, and where	9
07	7. Artificial intelligence	11
08	8. Cookies and similar technologies	11
09	9. Marketing	11
10	10. How we protect your information	12
11	11. How long we keep it, and deleting it	12
12	12. If something goes wrong	13
13	13. Seeing and correcting your information, and having it removed	13
14	14. Complaints	14
15	15. Children	14
16	16. Changes to this policy	14

01 1. Who we are, and our two roles

1.1 Cybermate is a trading name of Sycurus Australia Pty Ltd (we, us and Cybermate). Our platform is built for us by Synap AI Pty Ltd.

1.2 We have two roles. When an organisation (an employer, a school, a charity, a business) subscribes to Cybermate and adds its people, the organisation decides why and how their information is used, and we handle it for the organisation to provide the service. The organisation is responsible for telling its people what it collects and why. For information about our own customers and prospects (the organisation's administrators, billing contacts, people who sign up or enquire, and visitors to our website) we are responsible for the information ourselves.

1.3 If you use Cybermate through your employer or another organisation, you can also ask that organisation about its own privacy practices.

02 2. What we collect

The kinds of personal information we collect and hold depend on how you deal with us.

About	What we collect	Why
Your account	Your work email address, name, department, manager, job family, role in Cybermate, how you sign in, when you last signed in, and a protected form of your password if you use one	To let you sign in and to show you and your administrators the right things
Details you choose to give	Preferred name, pronouns, preferred time zone, position, work location, age range and gender. Time zone, department and work location are needed to use Cybermate; the rest are optional. We record exactly what you agreed to when you give an optional detail, and you can remove it at any time	To personalise training and show it at the right time. An organisation can switch off pronouns and gender, and then we stop asking for them and stop using them
Your training	The lessons written for you, your quiz answers and results, your progress, when you passed, and when your certificate is valid until	To teach and assess you, and to give your organisation a view of its training

About	What we collect	Why
Practice phishing emails	Whether a practice message was sent to you, delivered, clicked, reported, or an attachment opened, and when. We do not record anything you type on a practice page, because the page keeps nothing you enter	To teach you and to measure how well your organisation spots scams
Reports you make	The sender, subject and note you give when you report a suspicious email, and what we made of it	To help your organisation respond and to give you feedback
Dark web monitoring	If your organisation turns it on, the breaches your work email address appears in: the breach name, its date, the kinds of data exposed, and when we saw it	To warn you and your organisation when an address is exposed, so passwords can be changed
Your safety score	A score from 0 to 100 for your behaviour and knowledge, and a monthly copy of it	To show you and your organisation how well protected you are
Support	The questions and messages you send, replies, and files you attach, with your name, email address, role and organisation	To answer you
Secure messages	Only the encrypted message and its settings. We cannot read it. We record that you sent one, when, and its size, but not who it was for or what it said	To deliver the message and to keep the service safe
Using the platform	Your devices and sign-ins (device description, browser, IP address and approximate location), sign-in attempts, and an audit record of what was done and by whom	To keep your account safe and to show you and your administrators who has seen or changed information
Email we send you	Your address, what we sent, and whether it was delivered or bounced	To send the emails Cybermate sends and to stop sending to addresses that bounce
Organisations and administrators	The organisation's name, ABN, size, sector and optional address; the billing contact; payment records (card brand, last four digits and expiry, never the card number); invoices; and a registration number if a discount for a charity, not-for-profit or school was claimed	To bill, to give discounts, and to comply with tax law
Signing up and enquiries	Your email address, organisation name, the way you chose to pay, your IP address, and any details you give us when you enquire	To start your trial and respond to you

About	What we collect	Why
Our website	For visitors to www.cybermate.com.au: a random identifier kept in your browser, the pages you view (without the part of the address after a question mark), where you came from, your IP address, your browser, and how long a page was in view. If you later sign in, we link those visits to your account	To understand how people use the website and to help sign-up
Marketing	Your name, email address, phone number, company and role, how we met you, notes, and whether you agreed to hear from us	To tell you about Cybermate if you asked or agreed to hear from us

03 3. How we collect it

3.1 Mostly from you and from the organisation you use Cybermate through: you type it in, your administrator adds or imports your details (a name, a work email address and a department), or the platform records what you do. Your administrator never supplies the optional details in section 2: only you do.

3.2 From other sources: your sign-in provider (when you use Microsoft or Google sign-in we receive only your identifier, email address, whether the provider has verified it, and your name; we never see your Microsoft or Google password), the Australian Business Register (to look up an organisation name or ABN), and a breach data service (to check whether a work email address appears in known breaches).

3.3 If you do not give us information we need (for example the three required details), we may not be able to give you access to Cybermate.

04 4. What we use it for

4.1 We use personal information to provide Cybermate: to let you sign in, write and deliver your training, run practice phishing, warn you about exposed email addresses, show you and your organisation your results, answer your questions, send the emails the service needs (invitations, reminders, notices, invoices), bill your organisation, keep the platform secure, prevent misuse, meet our legal duties and improve the service.

4.2 We do not sell personal information. We do not use what your organisation's people do in Cybermate to advertise to them. We do not use it to train our own artificial intelligence models, because we do not train any.

4.3 We use website and marketing information to run and improve our website and to contact people who asked to hear from us or whom we may contact under the law. You can opt out at any time (section 9).

05 5. Who can see your information inside your organisation

5.1 You can see your own information, including your breach findings and who has looked at your data. Other people see only what their role allows.

- Your manager can see training progress for the people they manage. A manager does not see phishing results, breach findings or safety scores.
- Your organisation's administrators can see how far you have got in training, and totals for practice phishing with no names. Quiz answers and scores, and results with names, reach only the organisation's named security contact. Groups of fewer than five people are left out of phishing results so nobody can be picked out.
- Breach findings that are marked sensitive are never shown to an administrator or the security contact, and are never counted in an organisation's totals.
- Your support requests are private to you: your manager and administrators cannot read them.
- Everything done on your organisation's account is recorded, and your administrators and the security contact can see the record for people in your organisation.

5.2 Cybermate staff can see customer information only when that is needed to give support or keep the platform secure. When staff act as a user to help, the person sees a banner and the event shows in their own activity page. Direct access to the database is limited to a time-limited emergency account, and is recorded.

06 6. Who else handles your information, and where

6.1 We use the service providers below to run Cybermate. We disclose to each only what it needs for its job. The platform's database, files and backups are held with Google Cloud in Sydney, Australia. Some of the providers below may handle information outside Australia, including in the United States and other countries, and for some we cannot say in advance exactly where. We take reasonable steps to make sure they handle information in line with the Australian Privacy Principles, but we cannot control what a provider does once it holds information outside Australia.

Provider	What it does	What it receives
Google Cloud	Hosts the platform in Australia: database, files, backups, encryption keys, sign-in (Identity Platform) and voice for lesson narration (Text-to-Speech)	All the information the platform holds, encrypted. The text of a lesson section, which can address you by first name, for narration
Google Vertex AI and Anthropic	Artificial intelligence services that write personalised training, quiz questions, reminder wording and automatic answers to support questions	For training: your first or preferred name, department, role, work location, your organisation's name, and (to steer examples only) your age range, gender, pronouns and time zone. Never your surname or email address. For support answers: the text of your question
Stripe	Takes card payments and keeps stored cards	Your organisation's name, its administrator's email address, its identifier and ABN, invoice amounts, and card details that you type into Stripe's own form (we never receive the card number)
Mailgun	Sends our emails	The recipient's address and name, and the subject and body of each email
Twilio	Sends text messages for our own marketing	The mobile number and message of a marketing contact
Have I Been Pwned	Tells us whether an email address appears in known data breaches	One work email address at a time, with no name, role or organisation
bity.au	Shortens the links in practice phishing emails	The link, which carries your personal practice-message token
Australian Business Register	Looks up organisation names and ABNs	The organisation name or ABN typed in
Cloudflare	Domain name services for our domains	Internet address lookups, not your account information
Our own advisers and the authorities	Lawyers, accountants and insurers, and the courts or regulators where the law requires	What is needed for the purpose

6.2 Some Cybermate staff use an AI assistant to help work through support requests. The assistant is given the request, including your name, email address and organisation, for that purpose only.

07 7. Artificial intelligence

7.1 Cybermate uses artificial intelligence to write your training, quiz questions, reminder wording and automatic answers to Support questions. It can be wrong, even after our checks. It is general information for learning, not advice.

7.2 We send the AI services only what is described in section 6. Your organisation can switch off pronouns and gender, and then they are not sent. We check what the AI writes before you see it, and we do not use anything you do in Cybermate to train a model of our own.

08 8. Cookies and similar technologies

8.1 The Cybermate platform uses only first-party cookies it needs to work: to keep you signed in and to remember your organisation and, if you choose it, a trusted device for 30 days. It does not load advertising or tracking scripts from other companies.

8.2 Our public website runs a small analytics script of our own that keeps a random identifier in your browser for up to 13 months. It does nothing if your browser sends a Do Not Track signal, and it does not read anything you type into a form. You can clear it from your browser's settings or block it.

09 9. Marketing

9.1 We send marketing email and text messages only to people who have asked for them or whom the law allows us to contact. Every marketing message tells you how to stop them, and you can unsubscribe at any time. Messages the platform needs to send (an invitation, a reminder, a security notice, an invoice) are not marketing and continue while you have an account.

10 10. How we protect your information

10.1 We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, change or disclosure. They include keeping each organisation's information apart in the database, encrypting information in transit and at rest with keys we manage, requiring two-step verification for administrator accounts, limiting and recording staff access, an audit log of what is done on the platform, and card details being handled only by our payment provider.

10.2 No system is perfectly secure. We do not claim that an independent body has assessed our security.

11 11. How long we keep it, and deleting it

11.1 We keep personal information only as long as we need it for the purposes in this policy, or the law requires.

11.2 Training, practice phishing, reports and risk-score records are given an expiry date 18 months after they are created. Automatic removal of expired records is not yet switched on for every kind of record, so some may remain longer than 18 months until it is. We will update this policy when it is. In the meantime you can ask us to delete or de-identify your information at any time (section 13).

11.3 Some information is removed on a fixed schedule: secure messages after at most 8 days, uploaded people spreadsheets after 2 days, personal data exports after 7 days, and website analytics after about 13 months.

11.4 When a person's account is removed we replace their name, email address and other identifying details with a placeholder, so their records no longer identify them. We may keep email delivery records (which include the address an email was sent to), consent records, and audit records, for security, to show what was agreed, and to meet our legal duties. We keep invoices and payment records for 7 years because tax law requires it, and an organisation's audit log for the period set for that organisation (7 years unless it is changed).

11.5 Support requests and their files are kept for as long as we need to help you and for our records. Deleted information may remain in our backups for up to 35 days and in system logs for up to 7 days, and is then overwritten.

11.6 When an organisation stops using Cybermate we deal with its people's information as the Terms of Use say.

12 12. If something goes wrong

12.1 We keep a record of security incidents and follow a process to assess them. If we become aware of a breach of security affecting personal information we hold, we assess whether it is likely to result in serious harm. If it is, we tell the organisation whose information it is, so it can meet its own duties, and we notify the Office of the Australian Information Commissioner and the people affected where the Notifiable Data Breaches scheme requires us to.

13 13. Seeing and correcting your information, and having it removed

13.1 You can see and correct many of your details yourself on your profile page, and you can remove any optional detail you gave. The page shows what Cybermate holds about you, and the activity page shows who has looked at your information.

13.2 You can ask us for access to the personal information we hold about you, to correct it, or to delete it, by emailing support@cybermate.com.au. We may need to check who you are first. If you use Cybermate through an organisation, we may need to pass your request to that organisation, because it decides how your information is used and holds much of it. We will respond within 30 days.

13.3 If we refuse a request, we will tell you why in writing, as far as the law lets us, and how to complain.

14 14. Complaints

14.1 If you think we have breached the Australian Privacy Principles, email support@cybermate.com.au with the subject Privacy complaint, or write to us at 11/14-28 Blues Point Road, Mcmahons Point NSW 2060. We will acknowledge your complaint, look into it and reply in writing within 30 days.

14.2 If you are not satisfied with our response, you can complain to the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992).

15 15. Children

15.1 Cybermate is for people aged 18 and over. We do not knowingly collect information about children. A school programme for students is not offered, and if it is we will update this policy and put arrangements in place first.

16 16. Changes to this policy

16.1 We may update this policy. The current version and its date are on this page. If a change matters to you we will tell your organisation's administrators by email and in the platform.

This policy describes how Cybermate works at the date shown. If anything here is unclear, or you want to use any of your rights, email support@cybermate.com.au.