

DATA & PRIVACY POLICY

Thadus Group / Thadus CodeLabs

A plain-language account of every type of data Thadus collects, what it is used for, and what we will never do with it.

Last updated: August 2026

Applies to: thaduscodelabs.com, the Partner Portal, and the Thadus CodeLabs desktop application

Our core promise: We will never sell your name, email, or any identifiable personal information to anyone — not now, not ever. Our commercial activity is built entirely on anonymised, aggregated data that cannot identify any individual.

01 — OVERVIEW

Two products. Two different data footprints.

Thadus CodeLabs has two components with very different relationships to data. This policy covers both.

The Desktop App	The Partner Portal
The coding application students use day-to-day. Runs fully offline. When internet is available, it sends basic session information — which device is active, which centre it belongs to, and progress through the course. It does not send anything students type or create.	The online platform used by educators, admins, and Thadus staff. Collects account information, survey responses, monthly reports, and support conversations. Also stores the session data sent by the desktop app.

A few things we want to be upfront about:

The desktop app collects basic session data automatically whenever it is connected to the internet — including from devices being used without a valid licence. There is no in-app setting to turn this off.

We also want to be honest: the session data the app sends is not fully anonymous. While it does not include any student's name, the combination of a device identifier, centre name, and approximate location could in theory narrow to a small group in a very small deployment. We say this plainly rather than overstating our anonymisation.

02 — WHAT THE DESKTOP APP SENDS

Basic session and progress information.

When the app is connected to the internet, it sends session data to our servers. No student names, passwords, or content created by students is ever included.

What is sent during a session:

- A device identifier — a random code generated when the app is first installed. It identifies the machine, not the person using it.
- The centre's licence key — this identifies which organisation and location the device belongs to.
- Which type of event occurred — for example, the app opening, a module being viewed, a module being completed, or the session ending. The app also sends a regular check-in signal while it is open.
- The app version currently installed.
- Whether the device is licensed or unlicensed.
- The centre name.
- How long the session has been active.
- Which course and activity the student is currently on, and how far through it they are.

Approximate location:

The app does not send location data. However, every connection the app makes to our servers comes from an IP address, and our servers resolve that address to an approximate city and country using a third-party service. This gives admins a general sense of where devices are active. It is city-level only — not GPS, not an exact address.

Version checks:

The app periodically checks whether a newer version is available. These requests include the app version and licence details so we can confirm whether an update applies.

03 — WHAT THE PARTNER PORTAL COLLECTS

Account, programme, and support information.

The Partner Portal collects information needed to manage your programme, track outcomes, and provide support.

Account information

Created by Thadus when your partnership begins. Users do not self-register.

- Full name and email address
- Role — student, educator, admin, or partner manager
- Organisation and centre assignment
- Programme start date
- For student accounts: the supervising educator's email
- A device or location label if set by an admin

Login and access

- Passwords are stored in encrypted form only and are never visible to Thadus staff.
- Login sessions are managed securely and expire automatically.
- The licence key assigned to each user, organisation, or centre.
- Whether the app installer and licence file have been downloaded, and when.

Survey and programme data

- Pre-course survey (once per participant): career aspirations, STEM pathway interest, self-reported confidence and prior experience, and demographic information.
- Monthly reports (each cycle): self-reported module completion, change in confidence, and open-text responses.

Support and communications

- Support requests submitted through the portal — including the message content, priority, and status.
- Conversations with the in-portal AI assistant. Every message is stored and may be reviewed by Thadus staff for support and quality purposes.

Activity and milestones

- When students first interact with the portal.
- When the installer was first downloaded.
- Completion certificates issued per user per monthly cycle.

04 — WHAT WE DON'T COLLECT

Confirmed not collected.

The following have been verified against what the application actually does. These are facts about the software, not aspirational statements.

No student identity from the app	The app sends a device identifier and a centre licence key — nothing more. No student name, email, age, or personal identifier is ever sent from the app. Our systems link device data to an organisation, not to an individual person.
No student code or work	Whatever students type in the coding editor stays entirely on the device. None of it is sent to our servers at any point.
No camera or microphone	The app does not access the device camera or microphone. The avatar feature takes a screenshot of a portion of the app itself — it is not a webcam photo and is never uploaded.
No keystroke logging	Individual keystrokes are not recorded or transmitted. The app does not include any form of input monitoring.
No precise location	We know only the approximate city and country of a device, derived from its internet connection. No GPS coordinates, no street addresses.
No financial or biometric data	We do not handle payment cards or bank details. We collect no biometric data of any kind.

05 — HOW WE USE DATA

Everything has a clear purpose.

We do not collect data speculatively. Every piece of information we hold serves one of these purposes:

Running your programme

- ✓ Providing access to the Partner Portal
- ✓ Communicating with partner organisations
- ✓ Providing programme support and training
- ✓ Delivering monthly reports and completion certificates

Understanding app usage

- ✓ Knowing whether the app is being used at a centre
- ✓ Tracking programme-level course progress
- ✓ Identifying devices running without a valid licence
- ✓ Keeping the app up to date
- ✓ Giving admins a general view of where devices are active

Measuring and improving impact

- ✓ Understanding which parts of the programme are most effective
- ✓ Tracking outcomes across programmes and regions
- ✓ Supporting grant applications and funding reports
- ✓ Publishing anonymised programme statistics

Regional workforce intelligence

- ✓ Understanding youth career aspirations by region
- ✓ Identifying regional skills gaps
- ✓ Informing government education and employment policy
- ✓ Helping employers understand future regional talent

06 — ANONYMISED WORKFORCE & EDUCATION DATA

Our commercial model, explained plainly.

Free deployments for small NGOs and charities are funded by commercial data partnerships.

How it works: A commercial partner — such as a regional employer, government agency, or economic development organisation — wants to understand the career aspirations and skills landscape of young people in a specific region. Thadus deploys a free programme to a charity or NGO in that region. Over the programme period, we collect anonymised programme data. We deliver a Regional Intelligence report to the commercial partner. That payment funds the free deployment. **The commercial partner never receives any names, contact details, or records that could identify an individual.**

What commercial partners receive	What commercial partners never receive
✓ Aggregated statistics for a defined region	✗ Any student's name
✓ Career interest distributions across a cohort	✗ Any student's email or contact details
✓ Skills development trends	✗ Any individual student record

✓ Participation and engagement rates	✗ Any record that could identify a specific person
✓ Programme completion data	✗ Any data about the organisation's staff
✓ Demographic breakdowns — age ranges, gender	✗ The name of any organisation, without explicit written consent

07 — HOW AGGREGATED INSIGHTS WORK

The difference between population data and personal data.

What we might report	What we never report
✓ 42% of students in rural Region X are interested in healthcare careers.	✗ "John Smith from School ABC wants to become a nurse."
✓ Participation rates among female students aged 14–16 increased 28% over the programme.	✗ "Priya Sharma, age 15, completed modules 1–7."
✓ In this deployment, 67% of students had no prior exposure to coding.	✗ "These 45 students from St Joseph's Primary have no prior coding experience."
✓ The most common career aspiration in this cohort was engineering (31%).	✗ "Carlos Mendes listed engineering as his top career interest."
✓ Average course completion rate across the programme: 74%.	✗ "Student Amara did not complete modules 4 and 5."

08 — WHO CAN SEE WHAT

Clear access levels for every user type.

Access within the Partner Portal is strictly role-based. No organisation can see another organisation's data.

User type	Own data	Their students	Their org	Other orgs	Analytics
Student	Own only	No	No	No	No
Educator	Yes	Yes	No	No	No
Org admin	Yes	Yes	Yes	No	No
Thadus staff	Yes	Yes	Yes	Yes	Yes
Commercial partner	No	No	No	No	Anon. only

'Anon. only' — commercial data partners receive pre-processed, anonymised regional datasets only. Never raw data or anything linked to an individual.

09 — WHAT WE NEVER SELL

Some things are simply not for sale.

The following will never be sold, licensed, shared, or disclosed to any external party for any commercial purpose, ever.

X Names	X Email addresses	X Phone numbers
X Physical addresses	X Individual learning records	X Personal identities
X Student profiles	X Educator records	X Organisation contact lists
X Private communications	X Passwords or credentials	X Any identifiable record

This commitment is unconditional. It does not have carve-outs for 'trusted third parties,' 'service providers,' or 'business transfers.' If we ever faced a situation that required us to reconsider this, we would contact affected partners directly and seek explicit consent first.

10 — THIRD-PARTY SERVICES

Services that receive data in order to operate the platform.

Four external services handle data as part of running Thadus. We name them here with exactly what each receives.

Service	What it receives	Why
Supabase	All portal data — user accounts, survey responses, session data from the app, support conversations, and login records.	Hosting and securing the database and user authentication
Render	Standard server connection logs — request times and response codes. No user content.	Hosting the portal server
ip-api.com / ipinfo.io	IP addresses from app connections only, to convert them to a city and country.	Approximate device location for admin visibility
Email provider (SendGrid)	Name and email address of the recipient only.	Sending login credentials and programme notifications

We do not share data with advertising networks, analytics platforms, or data brokers.

11 — DATA SECURITY

How we protect what you share with us.

- Secure hosting:** All portal data is stored on Supabase. Data is encrypted at rest and in transit — it cannot be read by anyone who intercepts it.
- Access controls:** Users only see the data their role allows. Admin access to production data is limited and logged.
- Data retention:** Personal data is retained for the duration of your partnership and up to 24 months after. You can request deletion at any time.

No tracking scripts: The Partner Portal does not include advertising trackers, social media pixels, or any third-party behavioural tracking.

Anonymisation before sharing: Programme data is anonymised and aggregated by our team before it is compiled into any report. Raw records are never shared.

Breach notification: In the unlikely event of a data breach, we will notify affected partners within 72 hours and report to relevant authorities.

12 — YOUR RIGHTS

You are in control of your data.

We honour these rights for all users of the Partner Portal, regardless of where you are located.

Right to access: Request a copy of all personal data we hold about you at any time.

Right to correct: Ask us to correct any inaccurate or incomplete information we hold.

Right to deletion: Request that we delete your personal data. We will act within 30 days.

Right to portability: Request your data in a machine-readable format (JSON or CSV).

Right to object: Object to specific uses of your data, including use in anonymised regional reporting.

How to exercise your rights: Email neth@thaduscodelabs.com. We respond within 5 business days.

13 — FREQUENTLY ASKED QUESTIONS

Questions we hear most often.

Q: What does the desktop app actually send?

A: It sends a device identifier, the centre's licence key, and session information — which event type occurred, how long the session lasted, which course and activity is active, and how far through the course the student is. It does not send student names, what students type, or any personal information about the person using the app.

Q: The app has a photo feature. Does it use the webcam?

A: No. The avatar photo feature captures a portion of the app window on-screen — it is a screenshot of the app itself, not a webcam capture. The image is saved locally on the device only and is never sent to Thadus.

Q: Will a company buying Regional Intelligence be able to identify our students?

A: No. Regional Intelligence reports contain only aggregated statistics — percentages, averages, and trends across a cohort. They contain no names, no contact details, no individual records.

Q: Can a company find out which school or organisation we are?

A: No. We will never name a specific organisation, school, or community partner in any report provided to a commercial data partner without explicit written consent from that organisation's leadership.

Q: Are chatbot conversations stored?

A: Yes. Every message sent to and from the in-portal AI assistant is stored and linked to your account. These may be reviewed by Thadus staff for support and quality purposes. Please do not share passwords or sensitive personal information through the chatbot.

Q: What happens to our data when our partnership ends?

A: Personal information — names, emails, login records — is retained for up to 24 months then deleted. Anonymised programme data may be retained in de-identified regional datasets. You can request full deletion at any time by emailing us.

Q: Can students or parents object to data collection?

A: Yes. Contact neth@thaduscodelabs.com to request that a student's data is excluded from anonymised reporting datasets. The student can continue using the programme.

14 — CONTACT

Get in touch.

Have a question about this policy, want to exercise a data right, or just want to speak to a human? We respond within 5 business days.

Email: neth@thaduscodelabs.com

Organisation: Thadus Group — Thadus CodeLabs operates under Thadus Group, Brisbane, Australia