Trust and security

Why a school can trust EaseAcademia with its records and its pupils' data, how that data is protected, how the platform helps a school meet the Nigeria Data Protection Act, and the questions worth asking any provider.

Last updated · 19 October 2026

In short

A school holds some of the most sensitive information anyone keeps about a child: health notes, safeguarding concerns, home addresses, family phone numbers, fees owed and exam scores. Parents hand it over because they trust the school. When the school runs on EaseAcademia, part of that trust passes to us.

This guide explains how that trust is earned. It is written for proprietors, principals and data protection officers, and for the IT lead or trustee a school asks to check a provider. Every statement about EaseAcademia describes how the product works today. Where a protection has a limit, the limit is stated, and what we do not yet claim has a section of its own.

- **The school stays in charge.** The school is the data controller and EaseAcademia is its processor. The data is used to run the school and for nothing else. It is never sold, and children's data is never used for advertising or profiling.
- **Every door starts locked.** Each action is refused unless the person's role allows it, and each school's records are kept apart from every other school's.
- **The most sensitive writing is encrypted twice.** Everything is encrypted in transit and at rest, and 167 sensitive fields, from clinic notes to safeguarding records, carry a second layer of encryption of their own.
- **Nothing happens without a trace.** Actions, and attempts that were refused, are written to a sealed audit trail the school can search.
- **The law is built in.** The controls the Nigeria Data Protection Act expects are part of the product, and EaseAcademia's own duties are set out in a published data processing addendum.

What a school entrusts to us

Not all school data carries the same risk. A class list matters; a note about a child's medication or a safeguarding concern matters far more. EaseAcademia protects all of it, and adds layers as the sensitivity rises.

What it is	Examples	How it is protected
Everyday records	Names, classes, timetables, attendance, marks	Encrypted in transit and at rest, shown only to roles that need them, every change recorded
Family and contact details	Guardians' phone numbers and email addresses, home addresses, notes about a family	All of the above, and addresses and notes are encrypted field by field

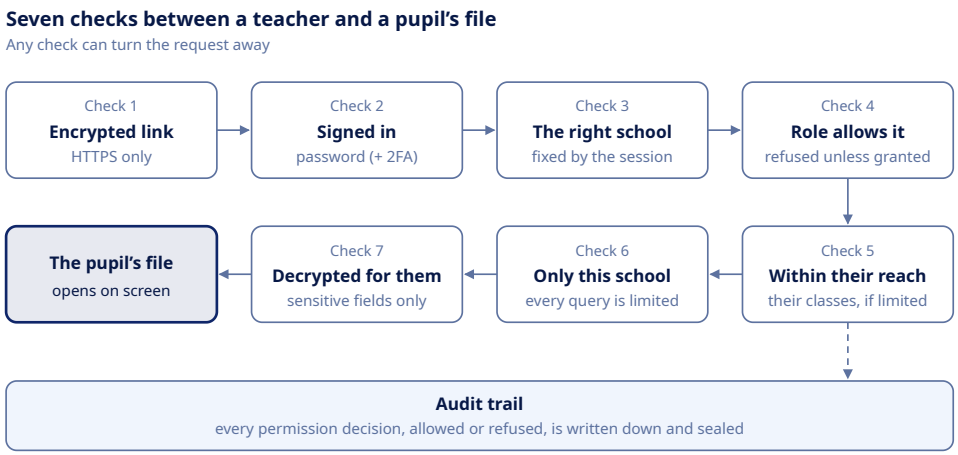
What it is	Examples	How it is protected
Money	Fee bills, payments, refunds, the school's prepaid credit	All of the above; card details are handled by Paystack and never stored by EaseAcademia, and every payment notice is checked against its signature
Sensitive personal data	Clinic visits and medication, safeguarding and discipline, staff grievances and disciplinary cases, recruitment notes	All of the above, and each field is encrypted on its own before it is stored
Files	Report cards, admission documents, photos, message attachments	Encrypted in storage, never public, opened only through links that expire

The principles behind every control

1. **Refuse unless allowed.** Access starts at nothing and is granted role by role. A mistake in setting up a role fails safe: someone is missing a screen, rather than seeing one they should not.
2. **Assume any one layer can fail.** Signing in, permissions, separation between schools, encryption and the audit trail are separate defences. Getting past one does not open the others.
3. **Refuse to run insecurely.** The live service will not start without its encryption key, its signing secrets, secure sign-in cookies and encrypted file storage. A configuration mistake stops the service instead of quietly weakening it.
4. **Check automatically, on every change.** The safeguards have automated checks of their own, which run before any change reaches a school.
5. **Say plainly what we do not do.** A trust document that lists only strengths is marketing. This one lists its limits too.

Seven checks between a person and a record

When a teacher opens a pupil's file, the request passes through each of these checks in turn. Any one of them can turn it away.



The path of one request. A failed check stops it there; every permission decision, allowed or refused, is written to the audit trail.

The sections below take each layer in turn, in enough detail to be checked.

Signing in

Most breaches start at the front door, so this is where the most care goes.

- **Passwords are never stored.** Only a one-way Argon2id hash is kept, so EaseAcademia can help someone reset a password but can never read it. A password needs at least eight characters with an upper-case letter, a lower-case letter, a digit and a symbol. Changing it requires the current one, and reusing it is refused.
- **Guessing locks the account.** Five wrong passwords within fifteen minutes lock the account for fifteen minutes. The lock is kept with the account, so restarting a server does not clear it, and the account holder is alerted in the app and by email.
- **Two-factor sign-in is available.** Staff, administrators and parents can add an authenticator app, which produces a six-digit code that changes every thirty seconds, with ten one-time recovery codes for a lost phone. There is deliberately no text-message or email code: both are weaker than the password they are meant to back up. Students and alumni sign in without a second factor.
- **A school can require it of its staff.** Once a school turns the requirement on, every member of staff (anyone holding a role there beyond pupil, graduate or parent) must set up an authenticator app. The school chooses a grace period of none, three, seven, fourteen or thirty days, and someone who joins later gets the same period from the day they join. Staff are told in the app and by email, and reminded the day before their deadline. After it, the only screen that opens for them is the one that sets it up, and while the school requires it they cannot switch it off. Only an account that already uses two-factor sign-in can change the setting.
- **A lost phone has a way back.** If a member of staff loses both phone and recovery codes, the school can reset their second factor, with a stated reason. Only the owner can reset an administrator, nobody in the school can reset the owner, and the school cannot reset an account the person also uses at another school. Every reset is recorded in the audit trail and emailed to the account holder.
- **Sessions are short-lived.** The pass that authorises each request lasts fifteen minutes. It is renewed with a token that is replaced on every use, stored on our side only as a hash, and can be withdrawn at any time. That

token sits in a cookie the page's own scripts cannot read, travels only over HTTPS, and is sent only to the sign-in service. Renewal requests from any other website are refused.

- **Reset links are single-use.** A reset link is stored only as a hash, works once, and expires after one hour. Using it signs the account out on every device.
- **Shared computers are covered.** A school office computer left alone signs itself out after ten minutes, with a one-minute warning first, and every hour asks whether the person is still there. Signing out wipes the cached pages and saved form drafts from that device.
- **Leavers lose access quickly.** Deactivating a member of staff stops their access within fifteen minutes at most, and changing a staff member's work email address signs them out everywhere.

What each person can reach

Signing in answers "who is this?". Everything after it answers "what may they touch?".

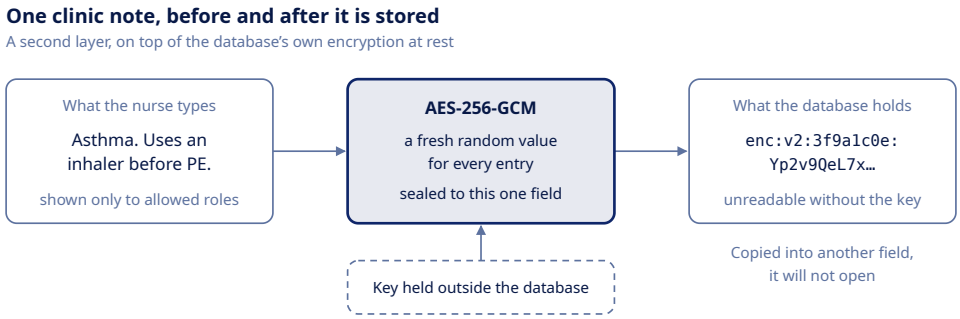
- **Every action is checked.** Each action in the school's portals is checked against the person's roles before it runs. If nothing grants it, it is refused, and the refusal is recorded.
- **Roles follow real jobs.** Schools start from ready-made roles and can build their own, such as Exams Officer or Head of Boarding, in a role builder that reads as plain sentences. Permissions are set per module and per action, and a permission for a module the school has not switched on cannot be granted at all.
- **Reach can be limited.** A role can be limited to particular classes or departments. A form teacher or subject teacher who tries to open a class they do not teach is turned away.
- **Each portal is separate.** The same person may be a member of staff and a parent. Each portal has its own set of actions, so acting as a parent never unlocks what that person can do as staff.
- **Changes take effect straight away.** When a role or a module changes, open screens are updated within seconds. Every change to who holds which role is recorded, and raises a security alert.

Keeping schools apart

One platform serves many schools, so the most important separation is between them.

- The school a request belongs to is taken from the person's signed session, not from anything their browser can choose. A request that names a different school is refused.
- The data layer adds the school to every query it runs, and refuses to run a school query that does not name one.
- Our own platform administration is a separate world, with its own sign-in, its own cookie and its own permissions. It is not a stronger version of a school account, and no school account can be raised into it.

Encryption, three layers deep



Field-level encryption: the note is readable in the clinic, and unreadable to anything that looks at the stored data.

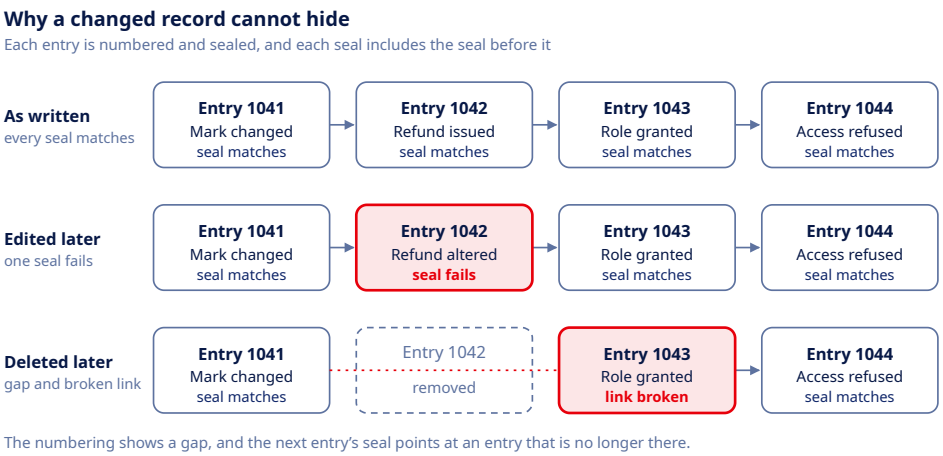
- **In transit.** All traffic between people's devices and the platform runs over HTTPS.
- **At rest.** The database and the file store are encrypted at rest. Every file is encrypted as it is written, and that requirement is signed into each upload's permission, so a browser cannot leave it out. The live service will not start if file encryption is switched off.
- **Field by field.** On top of that, 167 sensitive fields across 79 kinds of record are encrypted with AES-256-GCM before they are stored: clinic and medical notes, safeguarding and discipline records, staff grievances, disciplinary and performance cases, recruitment notes, family notes and addresses, admissions and transfer papers, exam questions and answers, and two-factor secrets. Each entry gets its own random value, each is sealed to the field it belongs to so it cannot be moved to another, and the key lives outside the database. Keys can be replaced without taking the service down.
- **The honest trade-off.** Encrypted text cannot be searched or sorted. Rather than encrypt a field and quietly break the search that depends on it, a short list of thirteen fields is kept searchable on purpose, such as message text and staff leave reasons, and each one is recorded with its reason in the same list that drives the encryption. An automated check stops any change in which that list and the code disagree.
- **Files are never public.** Every file opens through a signed link that expires: within an hour for most files, within a day for message attachments, and within seven days for profile photos and school logos, so that pages load quickly.

Money

- Parents' card details are entered with Paystack, the payment provider, and never reach EaseAcademia's servers.
- Every payment notice from Paystack is checked against a cryptographic signature before it is believed, so nobody can fake a payment by calling the platform directly.
- The school's prepaid credit is kept in a ledger in which every entry is signed and linked to the one before it, so a balance changed by hand does not check out.

A record that cannot be quietly changed

Prevention is never complete, so the platform is built to answer the question that follows any incident: who did what, and when, and was anyone turned away?



The audit trail's seals: an edited entry fails its own seal, and a removed entry leaves a gap and a broken link.

- **Written where the decision is made.** The audit entry is created at the same point that allows or refuses a request, so the trail includes attempts that were turned away: often the entries an investigation needs most.
- **Who, as they were then.** The person behind each action is recorded as they were at the time, so the trail still makes sense after someone changes role or leaves.
- **Sealed and chained.** Every record of a person's action, and every refused or failed attempt, is numbered in sequence and sealed with a keyed signature that includes the seal before it. Each day a digest of the chain is also written to file storage, apart from the database.
- **Yours to read.** A school's administrators can search their own trail by person, action, record and date, and export it as a spreadsheet file or as data.

Noticing when something is wrong

- Activity is summarised every minute into measurements per school and per kind of action, and alarms fire when a measurement crosses the limit set for it.
- Security alerts are raised for suspicious sign-ins, repeated guessing, changes to who holds which role, two-factor resets, audit trail exports and unusual activity.
- When an account is locked after repeated failures, or its two-factor sign-in is reset, the account holder is told in the app and by email.
- Sign-in cookies, session tokens and security headers are blanked out of the platform's request logs, so a log can never be used to take over a session.

When our team needs to look

Sometimes the only way to answer a support question is to see what the school sees. When that happens:

- the session is **read-only**: nothing can be created, changed or deleted;
- it covers **one school**, and needs a **stated reason** and a **fresh two-factor check** to begin;
- it **ends on its own**, after twenty minutes by default and one hour at most;
- it is **recorded**, with the number of actions taken, in the platform's own audit trail.

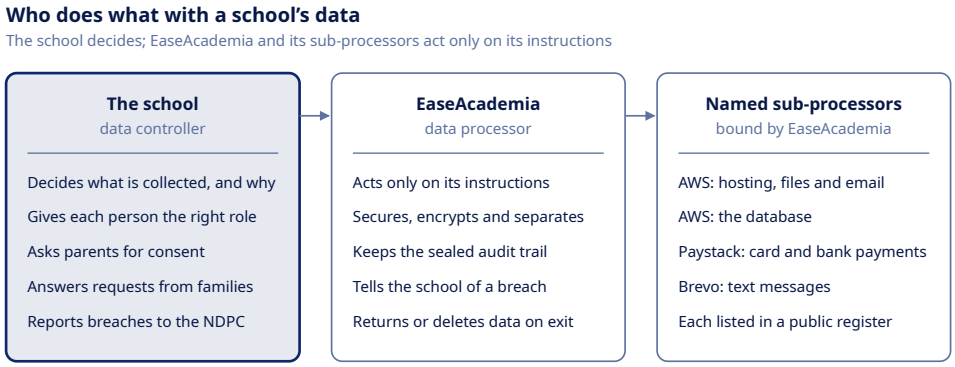
How the software is built

Most security failures are ordinary mistakes, not attacks. So the checks that matter run automatically on every change, and the ones that protect data stop the change rather than file a warning.

- Every change is scanned for secrets accidentally left in the code, and for known high-severity weaknesses in the software the platform relies on, including anything newly added.
- Automated checks confirm that the encryption list and the code agree, that limited roles stay limited, and that the database can be built from nothing, alongside more than 600 automated test files and 25 complete school journeys rehearsed end to end.
- Defaults are chosen to be safe when someone forgets: refusal rather than permission, and a service that will not start rather than one that starts weakened.

Who does what with a school's data

Data protection law gives most duties to the school, because the school decides what is collected and why. EaseAcademia carries its own share in writing, and binds the companies it relies on in turn.



Shared responsibility: the school decides, EaseAcademia acts on its instructions, and every sub-processor is named and bound in writing.

The full register of sub-processors, with what each one handles and where, is part of the data processing addendum. The platform is hosted with these established international providers, outside Nigeria, and the addendum commits EaseAcademia to appropriate safeguards for that transfer.

The NDPA, the NDPR and the GAID in plain language

Which rules apply today

Nigeria's first data protection rules were the **Nigeria Data Protection Regulation (NDPR) 2019**. They were followed by an Act of the National Assembly, the **Nigeria Data Protection Act 2023 (NDPA)**, which created the **Nigeria Data Protection Commission (NDPC)** to enforce it. In March 2025 the Commission issued the **General**

Application and Implementation Directive (GAID), which explains how the Act is applied in practice. Since the GAID took effect on 19 September 2025, the NDPR and its 2020 implementation framework no longer apply.

So when someone asks whether a school is "NDPR compliant", the question today is really about the NDPA and the GAID. They apply to every school that keeps personal information about pupils, parents or staff, whatever software it uses, and whether its records are on paper or online.

What the law asks of a school

The school is the **data controller**, so these duties are the school's. In plain terms, a school must:

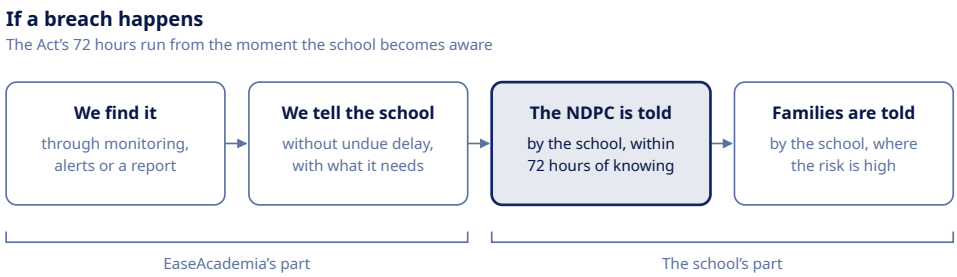
- collect only the information it needs, for a clear purpose and on a lawful basis, and keep it no longer than that purpose requires;
- obtain a parent's or guardian's consent where a child's information requires it, using suitable means to check age and consent. Under section 31 of the Act, a child is anyone under 18;
- take extra care with sensitive personal data, such as health information;
- keep all personal data secure, with suitable technical and organisational measures;
- let pupils, parents and staff see, correct, delete or obtain a copy of the information held about them, and object to its use, when they ask;
- report a personal data breach to the Commission within 72 hours of becoming aware of it, and tell the people affected directly where the risk to them is high (section 40);
- make sure any company handling the information on its behalf is bound in writing to protect it, and that information sent abroad stays properly protected.

Registration, a DPO and penalties

A controller that processes the personal data of more than 200 people in six months is treated as a **data controller of major importance**, under the Commission's 2024 guidance on section 44. Counting pupils, parents and staff, most schools pass that number. Controllers of major importance must register with the Commission, appoint a **data protection officer (DPO)** and file compliance audit returns.

Under section 48, a controller of major importance can be fined up to ₦10 million or 2% of its annual gross revenue for the previous year, whichever is higher. For other controllers, the figure is ₦2 million or 2%, whichever is higher.

The Commission is paying attention to education. In February 2026 it sent compliance notices to 649 higher institutions, asking within 21 days for their audit returns, their DPO's details, their registration and a summary of their technical and organisational measures. When a school is asked for that summary, this guide and the security page describe the platform's share of the answer.



If a breach happens: EaseAcademia tells the school without undue delay, so that the school can meet its own 72-hour deadline.

How EaseAcademia helps with each duty

No software makes a school compliant on its own. What EaseAcademia does is give the school the controls the Act expects, already built, and put its own commitments in writing. The right-hand column is what stays with the school, whichever provider it uses.

What the law expects	What EaseAcademia gives the school	What stays with the school
Collect only what is needed	Optional fields stay optional, and modules a school has not switched on collect nothing	Decide what to collect and why, and tell families in a privacy notice
Consent for children's data	Consent forms sent to parents in their portal, with each answer recorded with who gave it and when	Decide when consent is needed and what each form says
Security	Everything described in this guide	Give roles carefully, remove leavers promptly, and require two-factor sign-in for staff
Access and copies	Parents, pupils and staff see their own records in their portals; finance records and the audit trail export from the app; a complete copy of the school's data is provided on request	Answer each request in time
Correction	Staff can ask for changes to their profile and dispute entries on their professional record; the office corrects pupil and family records directly	Check each request and make the change
Deletion and retention	Administrators can delete records; former pupils' contact details are cleared automatically after seven years, or at once if they opt out; abandoned admission drafts are cleared	Set how long the school keeps each kind of record
Accountability	The sealed audit trail, searchable and exportable	Review it, and file the school's compliance audit returns
Breach reporting	Security alerts and monitoring, and a written commitment to tell the school without undue delay	Report to the Commission within 72 hours, and tell the people affected
A written processor agreement	A published data processing addendum; a counter-signed copy is available on request	Keep a signed copy on file

What the law expects	What EaseAcademia gives the school	What stays with the school
Transfers abroad	Named international providers, with appropriate safeguards committed to in the addendum	Say in the privacy notice that data is hosted abroad
Registration and a DPO	This guide, the addendum and the sub-processor register, ready for the school's filings	Register with the Commission if required, and appoint a DPO

This section is a plain-language summary, not legal advice. Take advice on your school's own obligations under the Act and the GAID.

Why this is stronger than common practice

Much of the personal data held by schools today does not live in a dedicated, protected system. It lives in the tools that were to hand when the school was small.

Common practice	The risk	On EaseAcademia
One shared administrator password for the school's software	Nobody can tell who did what, and people who leave keep the password	Everyone signs in as themselves, the school can require two-factor sign-in for all its staff, and a deactivated account stops working within fifteen minutes
Pupil lists and fee records in spreadsheets on personal laptops and flash drives	A lost device is a lost register, and nobody knows how many copies exist	One record, encrypted at rest, with files opened through links that expire
Class and fee matters handled in WhatsApp groups	Children's details and parents' numbers sit on personal phones, beyond the school's control	Messages and announcements go through the platform, only to the people each role allows
A server in the school office	Theft, power cuts and missed security updates	Professionally run cloud infrastructure, with the database and files encrypted at rest
Software in which every member of staff sees everything	A class teacher can open the fee ledger; a bursar can change a grade	Every action is refused unless a role allows it, and roles can be limited to particular classes
No record of changes	A dispute about an altered mark has no answer	A sealed audit trail of every change and every refused attempt
Health and safeguarding notes stored as plain text	One leaked copy of the database exposes the most sensitive notes a school keeps	Those notes are encrypted field by field, with the key held outside the database
No written agreement with the provider	Under the NDPA, the school carries its provider's risk alone	A published data processing addendum and a public register of sub-processors

Questions to ask any provider, including us

Question	EaseAcademia's answer
Who controls the data?	The school. EaseAcademia is its processor, under a published data processing addendum.
Do you sell the data, or use it for advertising?	No. Neither this website nor the portals carry advertising or analytics trackers.
How are passwords stored?	As one-way Argon2id hashes. Nobody at EaseAcademia can read a password.
Can we require two-factor sign-in?	Yes, for every member of staff, with an authenticator app and ten recovery codes and a grace period the school sets. Parents can turn it on for themselves. There is no text-message or email code.
What is encrypted beyond the disk?	167 sensitive fields across 79 kinds of record, each encrypted on its own with AES-256-GCM.
Can I see who changed a mark, and who was refused?	Yes. Both are in the school's audit trail, which the school can search and export.
Can your staff see our data?	Only through a support session that is read-only, limited to one school, needs a stated reason and a fresh two-factor check, ends within an hour and is recorded.
Who else handles our data?	AWS, Paystack and Brevo, each named with what it handles in a public register.
Can we take our data with us?	Finance records and the audit trail export from the app, and a complete copy of the school's data is provided on request. When a school leaves, it chooses whether its data is returned or deleted.

What we do not claim yet

A trust document is only worth reading if it is honest about its edges. These are the things a careful reviewer might ask about that EaseAcademia does not yet offer:

- **Certifications.** EaseAcademia does not hold ISO 27001 or SOC 2 certification.
- **An independent penetration test.** There is no third-party penetration test report to share.
- **Service guarantees.** There is no published uptime or recovery-time guarantee.
- **Required two-factor sign-in for parents.** A school can make two-factor sign-in compulsory for its staff, but for parents it remains their own choice.
- **Self-service export of everything.** A complete copy of a school's data is a request to support, not a button in the app.
- **School-set retention periods.** A school cannot yet set its own automatic deletion periods; records are removed by its administrators or on request.

When any of these changes, this guide will say so.

Reporting a concern

- **A security weakness:** write to security@easeacademia.com with the details and the steps to reproduce it. Good-faith research that respects people's privacy is welcome, and we ask for a reasonable chance to fix a problem before it is made public.
- **A data protection question or request:** write to dpo@easeacademia.com or privacy@easeacademia.com. Requests about a pupil's or a parent's records are passed to the school, because the school is the controller.
- **Anything else:** use "Report a problem", which is on every screen, or write to support@easeacademia.com.

The security page, the privacy policy and the data processing addendum give the formal detail behind this guide.

The latest version of this document is always at https://easeacademia.com/resources/trust-and-security.