

Privacy Notice

Phron Education Limited

Effective date: July 2026 | Version 2.0 | www.phron.co.uk

Phron Education Limited is a private limited company registered in England and Wales (company number 16870598). We build educational software for schools, multi-academy trusts and other education providers across the United Kingdom, helping them manage, organise and report on their data.

Much of the information we handle relates to children and to other sensitive matters, so we treat keeping it safe as a core responsibility. Data protection is built into the way we design our products, train our staff and run our business.

This notice explains what personal data we handle, why, and the choices and rights you have. It applies to everyone who comes into contact with our services: the school staff who use our platform, the customers and prospective customers we deal with, and visitors to our website and job applicants, as well as the pupils, parents and guardians whose data schools process through our systems.

If you have any questions, or you want to exercise a data protection right, you can reach our Data Protection Lead at dataprotection@phron.co.uk. We review this notice periodically and may update it in future.

1. Whether we are a controller or a processor

Our role under data protection law changes depending on the situation, and this determines who is responsible for the data.

1.1 When we act as a processor

When a school or trust uses our software, the school remains the data controller for all the pupil, parent and staff data it enters into our systems. We act as its processor: we handle that data only on the school's documented instructions and under our Data Processing Agreement (DPA).

We also support schools and trusts in meeting their own responsibilities as controllers, for example by helping them respond to subject access requests, providing a Data Protection Impact Assessment (DPIA) template, and assisting them if a data breach occurs. Schools can obtain a copy of the data they hold in our systems in a commonly used electronic format.

If you are a pupil, parent or member of school staff, the school decides how your data is used, so please refer to that school or trust's own privacy notice in addition to the information found here.

1.2 When we act as a controller

We are the data controller when we decide how and why data is used for our own purposes. That includes setting up and managing user accounts, dealing with sales, billing and customer support, sending marketing where you have opted in, running our website, recruiting staff, and, where our agreements with schools permit, producing anonymised benchmarks and analytics for the sector.

2. The personal data we handle

2.1 Data schools enter into our platform (we act as processor)

Schools decide what to record in our products, so the exact information varies from school to school and depends on the features in use. Broadly, it can include:

- **Pupil information**, such as identifying and demographic details, attendance and behaviour, assessment and progress, and pastoral, medical and safeguarding information.
- **Parent and guardian information**, such as contact and relationship details and emergency contacts.
- **School staff information**, such as role, contact, professional and employment details and, where relevant, vetting and safeguarding information.

Some of this is **special category data** under Article 9 of the UK GDPR, for example health information, ethnicity or data about special educational needs. Because the school is the controller, it is responsible for having a lawful basis and an Article 9 condition for processing it.

2.2 Data we collect directly (we act as controller)

The table below gives examples of the data we collect for our own purposes, why we collect it, and the lawful basis we rely on. It is illustrative rather than exhaustive, and the basis can differ depending on your relationship with us.

Who	Personal data	Purpose	Lawful basis
Platform users (school staff)	Account, profile and usage details	Running and securing accounts, authentication and support	Legitimate interests
Customers and prospective customers	Contact and organisation details	Sales, onboarding, contract management and customer communications	Contract; legitimate interests
Marketing recipients	Contact and organisation details	Sending you updates about our products and services	Consent
Website visitors	Technical and usage data about your visit	Operating and securing our website, and understanding in general terms how it is used	Legitimate interests
Job applicants	Application and eligibility information	Recruitment and employment administration	Legitimate interests; legal obligation

2.3 Data from public sources

To keep our information accurate and to improve our services, we sometimes draw on publicly available records, for example Department for Education performance and statistical data, published Ofsted inspection reports, and local authority directory and admissions information. We rely on our legitimate interests for this.

3. The legal grounds we rely on

When we act as a controller, we process personal data under one or more of these grounds in Article 6 of the UK GDPR:

- **Contract**: to deliver what we have agreed with schools and users, including giving access to our products and handling payments.

- **Legitimate interests:** to run and improve our business, for instance keeping our platform secure and communicating with customers, and producing anonymised benchmarks where our agreements with schools permit.
- **Legal obligation:** to meet our tax, employment, accounting and regulatory duties.
- **Consent:** where we ask for it, such as for marketing; you can withdraw consent at any time by emailing dataprotection@phron.co.uk.

Where special category data is processed on a school's behalf, the school (as controller) is responsible for identifying the Article 9 condition, usually the substantial public interest condition in Schedule 1 of the Data Protection Act 2018 for education and safeguarding. We may also process data to defend legal claims, or where the law otherwise requires it.

4. What we use personal data for

In short, we use personal data to:

- Provide, maintain and improve our software and related services
- Set up and manage user accounts and provide technical support
- Process data on behalf of schools, strictly on their instructions and under our DPA
- Keep customers informed about their accounts, service and updates
- Protect the security and integrity of our systems, including monitoring for unauthorised access
- Meet our legal and regulatory obligations
- Send marketing where you have opted in
- Produce anonymised, aggregated benchmarks and analytics for the education sector
- Recruit and administer our own staff

Our products continue to develop, so the specific ways in which data is used may change over time. Any such use will always fall within the purposes and lawful bases described in this notice; where it would not, we will update this notice first.

5. Artificial intelligence (AI) features

Some of our products include optional AI-assisted features that help school staff work more efficiently, for example by summarising or analysing information, drafting content for a member of staff to review, or reformatting existing records. Since these features process data that schools enter, we operate them as a processor, on the school's instructions. Whatever AI features a school chooses to use, the same safeguards apply:

- **Off by default and school-controlled.** Every AI feature is switched off unless a school chooses to enable it, and schools can turn each one on or off independently.
- **Human review.** AI output is decision-support only. Where it could affect a pupil, a qualified member of school staff must review and approve it before anything is recorded or shared, and AI-generated output is clearly labelled as such.
- **Your data is not used to train AI models.** We do not use school data, or AI output, to train or improve any general-purpose AI model, and we require our AI providers to configure their services with no training and no retention of that data.
- **Kept in the UK.** AI processing runs on UK-hosted infrastructure, and school data is not sent outside the United Kingdom for these features.

- **Protected and auditable.** We apply role-based access, pseudonymise identifiers in prompts where practical, keep an audit log of AI activity, and carry out a Data Protection Impact Assessment before enabling higher-risk features.

Since the mandatory human-review step, we do not make decisions that have a legal or similarly significant effect on any individual by automated means alone.

We assess our AI features, and the mitigations built into them by design, in a Data Protection Impact Assessment. These assessments are available to customers to support their own data protection assessments.

6. When we share data, and with whom

We do not sell personal data. We share it only in the limited situations below.

6.1 Sub-processors

We use a small number of trusted providers to deliver our services. Each is bound by contract terms that mirror our own obligations under the UK GDPR, so our data protection responsibilities flow down to them. Our principal sub-processors currently include:

Sub-processor	Purpose	Location	Safeguards
Microsoft Corporation (Azure)	Cloud hosting, infrastructure and platform services	United Kingdom	Pinned to UK Azure regions; ISO 27001 certified; Microsoft enterprise data protection terms
Microsoft Azure OpenAI Service	AI model processing behind our optional AI features (section 5)	United Kingdom	UK region only; configured for no training and no retention; ISO 27001, 27017 and 27018

Where we are contractually required to, we will notify schools of any change to contracted subprocessor under our DPA, giving them the chance to object before a new sub-processor is engaged.

6.2 Other disclosures

We may also disclose personal data where we are required to by law, regulation or a court order; where it is needed to bring or defend legal claims; where a regulator such as the ICO or the Department for Education requires it; or where it is necessary to protect the rights, property and safety of Phron or others.

6.3 Anonymised and aggregated data

Where our agreement with a school permits it, we use anonymisation and pseudonymisation to create aggregated, non-identifiable datasets from data processed through our products. We use these for sector benchmarking that helps schools understand their performance in context, for research and product development, and for statistical reporting. Once data has been properly anonymised it is no longer personal data under the UK GDPR, and we apply robust techniques so individuals cannot be re-identified.

6.4 Business transfers

If Phron, or substantially all of its assets, is ever acquired by or merged with another organisation, personal data may be part of what transfers. If that happens, we will tell affected individuals and make sure the new owner is bound by obligations consistent with this notice and the UK GDPR.

7. Where your data is kept

All personal data processed through our products, including the AI features in section 5, is stored and processed in the United Kingdom, on Microsoft Azure UK data centres. We do not transfer personal data outside the UK.

If this ever changes, we will put appropriate safeguards in place as required by Article 46 of the UK GDPR, such as the ICO-approved Standard Contractual Clauses, and update this notice. You are welcome to ask us about any safeguards in place.

8. How we protect data

We take security seriously and use appropriate technical and organisational measures to guard against unauthorised access, loss, damage or alteration. These include:

- Encryption of data in transit and at rest
- Role-based access controls and multi-factor authentication
- Regular vulnerability scanning and penetration testing
- Secure software development practices
- Data protection and security training for staff, at induction and annually
- DBS checks for staff who can access personal data
- Incident response and business continuity procedures
- Regular backups held within the United Kingdom
- Prompt removal of access when staff leave, and regular access audits

8.1 Standards and certifications

We are building our information security management in line with recognised standards and currently hold the following certifications:

- **ISO 27001**: information security management
- **ISO 9001**: quality management, reflecting our commitment to consistent quality
- **Cyber Essentials Plus**: the UK Government-backed scheme that guards against common cyber attacks

8.2 If a data breach happens

We keep a Security Incident Response Plan to detect, investigate and respond to breaches.

Where a breach affects personal data we process on behalf of a school or trust, we will notify that school or trust without undue delay, and in any event within 48 hours of becoming aware of it. This is to give them time to meet their own duty to report to the ICO, which must be done within 72 hours of the school becoming aware of the breach. We will give them enough information to meet their reporting duties to the ICO and, where necessary, to affected individuals, and we will investigate the incident, record it, and take corrective action. Where our Data Processing Agreement with a school specifies a shorter period, that shorter period applies.

For breaches involving personal data we control ourselves, we will report to the ICO within 72 hours where there is a risk to people's rights, and tell affected individuals where that risk is high.

If you think your data may have been affected, please email dataprotection@phron.co.uk straight away.

9. How long we keep data

We keep personal data only for as long as we need it for the purpose it was collected, subject to legal and regulatory requirements. As a general guide:

- **Pupil, guardian and school data (as processor):** kept in line with the school's own retention policy and instructions. When our contract ends, data is returned to the school (or securely destroyed at its direction) and permanently deleted from our live systems and backups within 90 days, unless the law requires otherwise.
- **Platform user accounts:** kept for the life of the contract and deleted within 90 days of the account closing.
- **Customer and prospective customer data:** up to 3 years from our last interaction, or sooner if marketing consent is withdrawn.
- **Website server logs:** up to 12 months.
- **Recruitment data:** 6 months after a recruitment decision, unless you agree to longer.
- **System and security logs:** up to 12 months for security monitoring, fraud prevention, safeguarding audit trails and compliance.
- **Financial and invoicing records:** 6 years from the end of the relevant financial year, to meet tax, accounting and Companies Act requirements.

10. Your rights

Under the UK GDPR you have the right to:

- **Access:** ask for a copy of the personal data we hold about you.
- **Rectification:** ask us to correct data that is wrong or incomplete.
- **Erase:** ask us to delete your data in certain circumstances.
- **Restriction:** ask us to limit how we use your data.
- **Portability:** ask for your data in a structured, machine-readable format.
- **Object:** object to processing based on legitimate interests, or to direct marketing.
- **Withdraw consent:** where we rely on consent, withdraw it at any time.

Important: if your data is held by us as a processor for a school, please make your request to the school first, as it is the controller. We will help the school respond under our DPA. For data we control ourselves, email dataprotection@phron.co.uk and we will reply within one calendar month.

11. Cookies and similar technologies

Our website and products use only essential and functional cookies. These are needed for the site and platform to work and cannot be switched off. They include session cookies that keep you logged in, security cookies that protect against cross-site request forgery, and preference cookies that remember your settings. We do not use advertising, marketing or third-party tracking cookies.

Separately from cookies, our web servers automatically record technical information about each visit, such as IP address, browser type, the pages requested and the time of the request. We use these logs to keep the site secure, diagnose faults and understand in general terms how the site is used, relying on our legitimate interests.

12. Children's data

Our products process children's data as part of the services we provide to schools, and we treat that data with particular care. We:

- Process children's data only as instructed by schools (as processor) and under our DPA
- Apply strict access controls so only authorised school staff can see pupil data
- Carry out Data Protection Impact Assessments where processing is likely to be high risk to children
- Use role-based, granular permissions so staff only see the data their role requires

13. Changes to this notice

We may update this notice to reflect changes in our practices, the law or our services. We will tell customers about material changes by email or through our products. The effective date at the top shows when it was last revised.

14. How to contact us

For any question about this notice, to exercise a right, or to report a possible breach, contact:

Data Protection Lead

Phron Education Limited

Email: dataprotection@phron.co.uk · Web: www.phron.co.uk

15. Complaints

If you are unhappy with how we have handled your data, please give us the chance to put it right first by contacting us using the details above. You also have the right to complain to the Information Commissioner's Office (ICO):

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
www.ico.org.uk · 0303 123 1113

Phron Education Limited is registered in England and Wales (company number 16870598).