GLOBAL PRIVACY POLICY

Live classes and recordings update | Updated 02 November 2026

Read this update first, then the complete original policy retained in this PDF. This additive update is effective from 02 November 2026.

Key points for learners

- During live classes, classmates may see your display name and hear or see your contributions, depending on settings and participation.
- Ordinary replays are replaced when the corresponding class is repeated in the next cycle; for example, the next Week 1 replay replaces the earlier Week 1 replay.
- Selected teaching sessions may stay in the video-lesson library. Identifiable student participation is removed where feasible or covered by separate, informed express permission for that reuse.
- The class notice explains the audience, available participation choices, source-copy retention and privacy contacts before recording.

1. What this update adds

This update explains live-class participation and recordings supplied by Mathein or academic partners as part of a Mathein-powered course, including St Paul's Academy where applicable. It applies when classes use Zoom or similar services and when recordings are made available in the App. The relevant course or class notice identifies the organiser and responsible privacy contacts.

All pages of the existing policy follow this update unchanged, including its collection limits, legal grounds, children's protections, security commitments, international-transfer safeguards, retention provisions for other data, privacy rights and contact details. Original dates and section numbers identify the earlier issue. These additions do not remove or relax an existing safeguard or authorise unrelated uses. Applicable country protections and mandatory law continue to apply.

2. Information visible live or captured in a recording

Depending on meeting settings and participation, instructors and classmates may see or hear a participant's display name, profile image, camera video, voice, public chat, questions, shared screen, files or other contributions. Recording settings determine which of these are captured. Turning off the camera alone does not necessarily prevent a name, voice or chat contribution from appearing.

The organiser and meeting provider may also process attendance, connection or meeting-administration information. This does not mean such information is shown to classmates. Joining a class does not authorise disclosure of unrelated account data, email addresses, phone numbers, home addresses, payment information, private messages or individual assessment records. Learners should avoid sharing real patient identifiers, confidential third-party information or unnecessary sensitive personal information during a class.

3. Purposes, recipients and responsibility

Live participation supports interactive teaching and questions. Ordinary replays support revision and access by authorised students who could not attend live. Their audience is the relevant enrolled course or class group disclosed in advance, together with authorised teaching and support personnel. Identifiable participation is not made available to every App user or the public merely because a replay is uploaded.

Mathein is responsible for personal information under its control in the Platform, including its recording-storage and access activities. The academic partner's responsibility for organising and recording a class depends on the actual arrangement. A partner may act independently, jointly or on behalf of another organisation for particular activities; branding alone does not decide the role. The class notice identifies the arrangement and the relevant contact. Zoom or comparable meeting, hosting and storage providers process information under the applicable service and privacy arrangements. Existing contractual and international-transfer safeguards continue to apply.

4. Ordinary replays: replacement at the next class cycle

An ordinary replay is removed from active App playback when the corresponding class is taught again in a new cycle and its replacement replay is published. For example, the new Week 1 replay replaces the previous Week 1 replay. Removal is tied to the corresponding lesson, not automatically to the beginning of any unrelated new course or cycle.

The course or class notice explains the expected cycle and playback access. If a cycle is delayed or discontinued, the replay's continued availability and retention are reviewed; the absence of a replacement does not itself justify indefinite retention of identifiable participation. Removal from App playback is distinct from deletion of Zoom source files, working copies or backups. Those copies are addressed below.

5. Selected classes kept as video lessons

Selected classes may be retained in a long-term or permanent video-lesson library for authorised learners, potentially including future course cycles. The intention to use a class in this way and the intended audience must be explained separately from the ordinary replay arrangement.

Where feasible, reusable lessons contain the instructor and teaching material with identifiable student participation removed, edited out or made genuinely non-identifying. Where identifiable student participation is to remain, we obtain separate, informed express permission for that reusable-lesson purpose before that use, together with any consent or guardian authorisation required by applicable law. General agreement to the App terms or participation in a live class is not treated as permission for permanent identifiable inclusion.

A permanent teaching library is not a blanket right to retain student personal information forever. Continued retention is reviewed for necessity, relevance, the disclosed purpose, permissions and applicable rights. Identifiable material must be removed, edited or otherwise addressed when continued retention or use is no longer justified. Removing an ordinary replay does not automatically authorise moving it into the permanent lesson library.

6. Advance notice, legal grounds and participation choices

Before recording starts, the responsible organiser provides a clear notice explaining what will be captured, the purposes, intended viewers, ordinary replay replacement or selected-lesson use, relevant retention criteria, responsible parties and available choices. Each processing activity must have the legal ground or consent required in the applicable country. Attending the class, accepting general terms or granting a camera/microphone device permission does not replace any legally required recording or sharing consent.

The organiser explains available ways to participate without identifiable inclusion, which may include an agreed display name, camera and microphone controls, private questions, instructor repetition of a question without identifying its author, or editing before publication. The actual options and any limitations are explained before the learner chooses how to participate. A learner is not required to agree to unnecessary identifiable recording or reusable-lesson use as a condition of unrelated learning services. Requirements for children or younger users under the existing policy remain in force.

7. Source files, working copies, backups and retention

The replacement rule governs ordinary App replays. The responsible organiser separately identifies a necessary period for Zoom source files and editing or transfer copies, including any limited period needed to check a successful upload, correct an error or handle a legitimate request. A source file should not be retained merely because another copy is stored in the App. Class notices must explain the applicable periods or criteria; this document does not invent an unconfirmed number of days or imply that App removal automatically deletes every source copy.

Ordinary source and working copies that are no longer necessary are deleted or made genuinely non-identifying. Selected reusable-lesson masters are distinguished from ordinary replay working files and remain subject to the preceding safeguards. Restricted backups follow the applicable backup and deletion arrangements in the original policy. Any legal hold must be justified and limited to its legal purpose, not used to continue ordinary playback or create a new lesson-library purpose.

The original policy's general account, learning-data, payment, support and security retention rules remain unchanged for those data. A general learning-data period is not automatic permission to keep every identifiable class replay until that period expires despite the specific replacement rule.

8. Privacy requests, permission withdrawal and safeguards

The access, correction, deletion, complaint and other rights described in the original policy remain available. Where consent is relied upon, a learner may withdraw it through the applicable privacy contact. Withdrawal does not retrospectively invalidate processing that was lawful before withdrawal. Requests affecting a group recording are assessed for removal, editing, blurring, audio removal, restriction or other appropriate action, taking account of applicable law and others' rights. We explain the outcome and any lawful limit rather than promising that every copy can always be erased immediately.

Appropriate access controls, authorised-use restrictions and existing security and transfer safeguards apply to recordings. Students must respect the class rules and must not make unauthorised recordings, redistribute replays or share playback links outside the permitted audience, subject to legal rights and approved accessibility arrangements. These restrictions are not a guarantee that copying is technically impossible and do not waive a learner's privacy rights or remedies.

9. Separate purposes are not bundled into class attendance

Public release, advertising, promotional use, a new audience outside the disclosed group, or use of identifiable recordings to train general-purpose AI models is not authorised by this live-class update. Any such proposal needs a separate lawful assessment, clear notice and any required specific consent. If transcription, AI summaries or other processing is proposed, the notice must explain the actual information, provider and purpose and the appropriate legal process must be followed before use. All existing restrictions on advertising, sale of data and AI processing remain unchanged.

10. Country supplements and contacts

Read this update with the complete Global Privacy Policy reproduced below and the country supplement applicable to the learner. A country supplement or mandatory law may require additional notices, legal grounds, consent, language provision, youth protections, response procedures or transfer safeguards. Those requirements are not reduced by this update.

Mathein The Learning Company UK Ltd, 25 Strone Park, Dundonald, Belfast, Northern Ireland, BT16 1UW, United Kingdom. Privacy: privacy@matheinlearning.com. Support: support@matheinlearning.com. The class notice should also identify the relevant academic partner's privacy contact.

Existing policy follows unchanged

The original policy pages follow this update in full. The original issue date is retained as a historical identifier. The original section numbering and any original appendix are also preserved. The updated PDF bookmarks distinguish this update from the unchanged original policy.

Current legal publication points: Privacy Centre | Master Terms

MATHEIN LEARNING PLATFORMS

GLOBAL PRIVACY POLICY

For Mathein-Owned, Partner-Branded and White-Label Learning Applications

Company	Mathein The Learning Company UK Ltd
Document Type	Global Privacy Policy
Applies To	All Mathein-owned, partner-branded and white-label learning applications, websites, portals and related services that link to this policy
Current App Example	NCLEX with Fr. Josis
Last Updated	04 July 2026

This Global Privacy Policy contains common privacy terms. Country-specific privacy policies or supplements remain separate documents and apply in addition to this Global Privacy Policy where relevant.

Contents

1. 1. Introduction
2. 2. Who We Are: Data Controller, Data Fiduciary and Platform Operator
3. 3. Scope of this Policy
4. 4. Information We Collect
5. 5. No Third-Party Advertising and No Use of Android Advertising ID
6. 6. How We Collect Information
7. 7. Why We Use Personal Information
8. 8. Legal Bases and Regional Processing Grounds
9. 9. AI Processing and Automated Feedback
10. 10. Children and Young Users
11. 11. Cookies and Similar Technologies
12. 12. Payments, App Stores and Billing Providers
13. 13. Data Sharing and Service Providers
14. 14. International Data Transfers
15. 15. Data Retention
16. 16. Your Privacy Rights
17. 17. Account Deletion and Data Removal
18. 18. Security Measures
19. 19. Changes to this Policy
20. 20. Contact Information

1. Introduction

This Global Privacy Policy explains how Mathein The Learning Company UK Ltd ("Mathein", "we", "our", "us") collects, uses, stores, discloses, transfers, and protects personal information when individuals access or use any mobile application, website, portal, dashboard, learning platform, assessment tool, AI-evaluation service, payment flow, or related digital service developed, operated, hosted, licensed, or white-labelled by Mathein.

Our applications and services may be presented under different brand names, product names, logos, app-store listings, domain names, or partner names. Examples may include NCLEX with Fr. Josis and other current or future Mathein-powered learning applications. Where this policy refers to the "App", the "Platform", or the "Services", it means any current or future Mathein-owned, Mathein-operated, Mathein-hosted, partner-branded, or white-label learning service that links to this policy, unless a separate product-specific privacy notice expressly states otherwise.

This Global Privacy Policy contains the common privacy terms that apply across our Platform. Country-specific privacy policies or supplements may provide additional rights, response times, legal bases, contact details, grievance mechanisms, regulator information, or local legal requirements for users in particular countries. Where a country-specific policy or supplement applies, it should be read together with this Global Privacy Policy.

Mathein respects your privacy and is committed to handling personal information lawfully, fairly, transparently, securely, and in a way that supports learners, educational partners, and platform users across all jurisdictions where the Platform is made available.

2. Who We Are: Data Controller, Data Fiduciary and Platform Operator

Mathein The Learning Company UK Ltd is the company responsible for operating the Platform and for determining how personal information is processed through the Platform, except where a separate agreement or product-specific privacy notice expressly identifies another organisation as the controller or joint controller for a specific processing activity.

For users in the United Kingdom, the European Economic Area, Canada, and most other regions, Mathein The Learning Company UK Ltd normally acts as the data controller for personal information processed through the Platform.

For users in India, Mathein normally acts as the Data Fiduciary for personal data processed through the Platform, and service providers such as cloud, payment, communication, analytics, and AI providers act as Data Processors where they process personal data on our behalf.

Educational institutions, training providers, content owners, publishers, tutors, academic partners, white-label customers, or other organisations may provide branding, course content, learner groups, or institutional access. Where such a partner independently determines the purpose and means of processing personal information, that partner may act as an independent controller or joint controller for those specific activities. In that case, additional privacy information may be provided by that partner.

Contact details for Mathein are provided at the end of this policy.

3. Scope of this Policy

This policy applies to the common privacy practices used across the Platform, including:

- Android mobile applications distributed through Google Play;

- iOS mobile applications distributed through the Apple App Store;
- web applications and websites operated by Mathein or linked from a Mathein-powered application;
- partner-branded and white-label mobile applications;
- academic partner portals, staff dashboards, administrator dashboards, learner dashboards, and reporting tools;
- course discovery, enrolment, learning, practice, mock-exam, assessment, result, review, flashcard, notification, and support features;
- AI-evaluation workflows used to review descriptive answers, uploaded answer sheets, images, diagrams, or other permitted learner submissions;
- purchases, billing, tax calculation, invoices, receipts, refunds, subscriptions, wallet credits, in-app purchases, or other payment-related functions; and
- communications, feedback, support requests, marketing consent, service notifications, security, fraud-prevention, and analytics activities.

This Global Privacy Policy is intended to provide the common baseline. It does not replace country-specific policies where local law requires extra notices or rights. Country-specific policies and supplements listed on the Mathein legal webpage remain separate documents and should be read in addition to this Global Privacy Policy.

4. Information We Collect

We collect only the categories of personal information that are reasonably necessary to provide, secure, improve, support, and bill for the Platform. The exact information collected may vary depending on the app brand, country, course, payment method, account type, learner age, device, and features used.

A. Account, Identity and Contact Information

- Name;
- email address;
- phone number, where provided or required for support, verification, or account recovery;
- parent or guardian email address, where applicable;
- profile picture, where voluntarily uploaded;
- country, region, province, state, or age-range confirmation where needed for legal, tax, age-appropriate access, fraud-prevention, or platform configuration purposes; and
- login identifiers, authentication method, and account status.

B. Billing, Tax and Payment-Related Information For purchases, billing, invoicing, refunds, tax compliance, and fraud prevention, we may collect or receive:

- country;
- state, province, region, or similar tax location information where required;
- street address, address line 2, city, locality, postal code, or ZIP code where provided or required;
- course, bundle, plan, tier, wallet, subscription, or product purchased;
- transaction ID, order ID, receipt status, payment status, currency, amount, discount, coupon, tax amount, refund status, and invoice or receipt link;
- customer or payment reference identifiers from providers such as Stripe, Google Play Billing, Apple in-app purchase systems, banks, wallets, or other regulated payment providers; and
- payment risk, fraud-prevention, dispute, refund, or chargeback information.

We do not store full payment-card numbers or CVV codes. Card and regulated payment details are processed by payment providers.

C. Learning and Academic Activity When learners use courses, practice sets, mock exams, assessments, flashcards, reviews, or AI-enabled features, we may process:

- courses, bundles, subjects, institutions, exams, tiers, plans, and enrolment details;

- practice sessions, mock exams, attempts, scores, progress, completion status, time taken, bookmarks, flags, flashcards, answer history, and performance metrics;
- MCQ selections, typed descriptive answers, short answers, diagram responses, uploaded answer sheets, images, handwriting, documents, audio or video submissions where permitted by the course design;
- model answers, explanations, grading criteria, rubrics, AI configuration, AI scores, AI-generated feedback, and review-chat context; and
- learner feedback, question suggestions, ratings, and support comments.

D. Technical, Device and Usage Data We may collect technical information necessary to operate, secure, diagnose, and improve the Platform, including:

- IP address;
- device type, model, operating system, browser type, app version, language, time zone, and platform identifiers;
- app activity logs, login logs, page or screen events, crash logs, diagnostic logs, and error reports;
- cookie identifiers or similar technologies for web-based services;
- device identifiers used for security, fraud prevention, app integrity, anti-abuse, analytics, or crash diagnostics; and
- Google Play, Apple, or device information required to verify purchases, prevent fraud, maintain app integrity, or comply with app-store requirements.

Unless a specific feature clearly requests it and you grant any required permission, we do not collect precise GPS location. We may infer approximate country or region from billing information, IP address, app-store region, account settings, or user selection when needed for taxation, legal compliance, language, content access, security, or fraud-prevention.

E. Communications, Support and Preferences We may collect:

- support enquiries and complaint details;
- emails, messages, feedback forms, survey responses, and ratings;
- notification preferences and communication preferences;
- consent records and legal acceptance records; and
- records of service emails, verification emails, password reset emails, parental-consent communications, or other essential account communications.

5. No Third-Party Advertising and No Use of Android Advertising ID

The Platform is a learning, assessment, and evaluation service. We do not integrate third-party advertising networks for targeted advertising, and we do not use the Android Advertising ID for advertising or cross-app tracking.

Some apps may display internal course promotions, coupons, bundle offers, institutional notices, or service announcements. These are part of the learning and platform-service experience and are not third-party ad-network tracking. We do not sell personal information, share personal information for targeted advertising, or track users across third-party services for advertising purposes.

6. How We Collect Information

We collect information through:

- direct interactions, such as account creation, login, profile updates, course enrolment, test attempts, uploads, support requests, feedback, complaints, and consent choices;

- automated technical collection, such as app logs, crash logs, analytics, cookies, security logs, and app integrity checks;
- payment providers, app stores, banks, wallets, or payment gateways when a purchase, refund, verification, or payment-status check occurs;
- AI-evaluation workflows when answer text, images, documents, or other permitted submissions are securely transmitted for automated feedback or scoring;
- academic partners, institutions, tutors, publishers, or white-label customers where they lawfully provide course, enrolment, learner group, staff, or access information; and
- third-party service providers who support authentication, cloud hosting, email, analytics, payments, security, AI processing, app-store verification, or support operations.

7. Why We Use Personal Information

We use personal information for the purposes described below. The lawful basis or legal ground may differ depending on your country and the applicable country-specific policy.

A. To Provide and Operate the Services We use personal information to:

- create, verify, maintain, and secure accounts;
- authenticate users and manage login sessions;
- deliver courses, lessons, practice sets, mock exams, live classes, flashcards, results, and learner dashboards;
- provide staff, partner, academic, and administrator dashboards;
- evaluate MCQ, descriptive, image-based, uploaded, or other permitted answer types;
- generate AI scoring, AI feedback, review summaries, and learning insights;
- track progress, completion, access rights, subscription or validity periods, and entitlements;
- send essential service notifications, security alerts, payment confirmations, password resets, parental-consent requests, and account messages; and
- provide support, complaint handling, error recovery, and customer service.

B. For Payments, Billing, Tax and Financial Compliance We use personal information to:

- process payments, subscriptions, wallet credits, app-store purchases, refunds, and disputes;
- validate transactions and prevent payment fraud;
- apply coupons, discounts, referral offers, institutional access, or bundle pricing;
- issue receipts, invoices, tax documents, and billing history;
- comply with VAT, GST, sales tax, accounting, audit, consumer, and financial-record obligations; and
- reconcile payments with payment providers, app stores, and banks.

C. For AI Evaluation and Learning Feedback We use learner submissions, answer content, model answers, rubrics, scoring criteria, and related course context to provide automated or AI-assisted feedback and scoring. AI evaluation is used to support learning and assessment practice. It is not used to make legally significant decisions about users.

D. For Security, Fraud Prevention and Abuse Prevention We use information to detect, prevent, and investigate unauthorised access, cheating, misuse, fraud, payment abuse, account compromise, suspicious activity, technical attacks, policy violations, and service disruption.

E. For Analytics, Diagnostics and Improvement We use information to understand platform performance, fix bugs, diagnose crashes, improve usability, improve course delivery, analyse feature usage, maintain service quality, and plan future improvements. Where local law requires consent for analytics or cookies, we will request consent or provide appropriate controls.

F. For Marketing and Optional Communications We may send promotional messages, offers, course recommendations, or partner announcements only where permitted by law and, where required, with your

consent. You can withdraw marketing consent at any time. Essential service messages may still be sent even if you opt out of marketing.

G. For Legal, Compliance and Governance Purposes We use information to comply with applicable laws, app-store requirements, tax obligations, audit obligations, court orders, regulator requests, law-enforcement requests, complaints, dispute resolution, and enforcement of our terms and policies.

8. Legal Bases and Regional Processing Grounds

Depending on your location, our legal basis or processing ground may include:

- contract or performance of a service requested by you;
- consent, including consent for account creation, optional cookies, optional marketing, and parental or guardian consent where required;
- legitimate interests, such as platform security, fraud prevention, service improvement, analytics, support, diagnostics, and operation of a learning platform, provided those interests are not overridden by your rights;
- legal obligation, such as accounting, tax, fraud-prevention, age-related, regulator, consumer-protection, or record-retention duties;
- implied consent or deemed consent where applicable local law recognises it for necessary platform functions; and
- other legal grounds set out in the relevant country-specific policy or supplement.

Where country-specific law requires a different legal basis, additional consent mechanism, local notice, or response procedure, the relevant country-specific policy or supplement applies in addition to this Global Privacy Policy.

9. AI Processing and Automated Feedback

Some courses and assessments use AI-assisted evaluation. This may involve securely processing answer text, uploaded answer images, diagrams, handwritten answer sheets, rubrics, model answers, scoring criteria, explanations, and relevant course context through AI service providers such as OpenAI or similar processors.

We aim to ensure that:

- only the information reasonably necessary for evaluation is transmitted;
- submissions are transmitted through encrypted channels such as HTTPS/TLS;
- AI providers process submitted content under contractual or service-provider restrictions;
- submitted content is not used for targeted advertising;
- AI feedback is used to support learning, practice, review, and formative evaluation;
- AI outputs are not used to make legally significant decisions about users; and
- where provider controls are available, they are configured so that submitted learning content is not used to train public AI models.

AI-generated feedback may be imperfect. Learners should treat AI feedback as learning support, not as professional, medical, legal, migration, financial, or employment advice. For regulated examinations, professional qualifications, or institutional decisions, users should rely on the rules and official guidance of the relevant awarding body or institution.

10. Children and Young Users

The Platform is generally designed for learners aged 13 and above, unless a specific app, course, institution, or country-specific policy applies a higher age threshold.

Under 13 We do not knowingly process personal information of users under 13 unless a specific lawful child-access model, school/institutional framework, or guardian-controlled arrangement is enabled and permitted by applicable law. If we discover that a user under 13 has provided personal information without appropriate authorisation, we will take reasonable steps to delete or restrict the account and associated personal information.

Ages 13 to 17 For users aged 13 to 17, parental or guardian involvement may be required depending on the country, course, payment method, institution, or feature. We may collect a parent or guardian email address where needed for supervision, consent, safety, or compliance.

We do not knowingly use harmful or addictive design patterns directed at children, do not use children's personal information for targeted advertising, and do not use the Android Advertising ID for child-directed advertising.

Country-specific rules may apply, including requirements for guardian consent, grievance officers, response times, or additional child-safety notices. These are addressed in the relevant country-specific policy or supplement.

11. Cookies and Similar Technologies

Web versions of the Platform may use cookies, local storage, pixels, SDK identifiers, or similar technologies to:

- keep users signed in;
- remember preferences;
- secure accounts and detect abuse;
- operate essential website functions;
- analyse service performance;
- diagnose crashes and technical issues; and
- improve user experience.

Where required by law, we provide cookie notices or consent controls for optional cookies and analytics. Essential cookies or local storage needed for security, login, payment, or core platform functionality may operate without optional consent where permitted by applicable law.

12. Payments, App Stores and Billing Providers

Payments may be processed through third-party payment providers and app-store systems, including Stripe, Google Play Billing, Apple in-app purchase systems, banks, wallets, or other regulated payment providers used by a particular app or country.

Payment providers may process card details, payment authentication, fraud checks, transaction authorisation, refunds, chargebacks, receipts, tax data, and payment-risk information. Mathein receives limited payment-related information required to confirm purchases, unlock access, issue receipts, comply with accounting and tax obligations, prevent fraud, resolve disputes, and provide billing history.

We do not store full card numbers or CVV codes. Users should also review the privacy notices of the relevant payment provider or app store where applicable.

13. Data Sharing and Service Providers

We share personal information only where necessary for the purposes described in this policy, or where required by law. Categories of recipients may include:

A. Cloud, Backend and Authentication Providers Providers such as Firebase, Google Cloud, or similar services may support hosting, authentication, databases, analytics, crash diagnostics, storage, app integrity, security, and cloud operations.

B. Payment and Billing Providers Providers such as Stripe, Google Play, Apple, banks, wallets, and payment gateways may process payments, refunds, fraud checks, receipts, tax information, disputes, and transaction verification.

C. AI Evaluation Providers AI providers such as OpenAI or similar processors may process learner answers, uploaded answer content, rubrics, and related materials for AI evaluation, scoring, review, and feedback.

D. Communications Providers Email, SMS, push-notification, and support providers may help us send verification codes, password resets, service notices, support messages, legal notices, feedback requests, or marketing messages where permitted.

E. Academic, Institutional and White-Label Partners Where a learner is enrolled through an institution, school, college, tutor, publisher, training provider, academic partner, or white-label customer, relevant information may be shared under contract so that the partner can provide content, support, learning services, reporting, access management, or learner assistance. We share only what is reasonably necessary for the relevant learning or institutional purpose.

F. Legal, Regulatory and Safety Recipients We may disclose information where required to comply with law, enforce our terms, protect rights, investigate fraud or abuse, respond to court orders, respond to regulators, handle complaints, or protect users and the Platform.

We do not sell personal information. We do not share personal information with third-party advertising networks for targeted advertising. We do not track users across third-party services for advertising purposes.

14. International Data Transfers

Because the Platform is cloud-based and may be used internationally, personal information may be stored or processed in countries other than your country of residence. These may include the United Kingdom, the European Union, Canada, the United States, India, and other jurisdictions where Mathein, its service providers, or its partners operate.

Where required by applicable law, we use safeguards such as:

- contractual protections and data processing agreements;
- Standard Contractual Clauses or equivalent transfer mechanisms;
- the UK International Data Transfer Addendum or other UK transfer safeguards;
- adequacy decisions where applicable;
- Quebec Law 25 contractual measures where applicable;
- DPDP-compliant processor arrangements where applicable;
- encryption in transit and at rest where supported;
- access controls, audit controls, and security monitoring; and
- due diligence on service providers and processors.

Country-specific transfer rules may be described in the relevant country-specific policy or supplement.

15. Data Retention

We retain personal information only for as long as reasonably necessary for the purposes described in this policy, including service delivery, learning records, account management, billing, legal compliance, fraud prevention, audit, dispute resolution, tax, regulatory obligations, and security.

Unless a country-specific policy, legal requirement, contractual obligation, or product-specific notice states otherwise, our standard retention approach is:

Data Type	**Indicative Retention Period**
Account information	For the active account period plus up to 3 years, unless a longer or shorter period is required by law or agreed in a country-specific policy.
Learning and test data	For the active account period plus up to 3 years, unless earlier deletion is requested and no legal or operational retention reason applies.
Payment and transaction data	Usually 6 to 7 years, depending on tax, accounting, audit, chargeback, legal, and country-specific requirements.
Support communications	Usually up to 24 months, unless needed for legal, complaint, safety, or dispute purposes.
Security, fraud-prevention and audit logs	For as long as reasonably necessary for security, fraud-prevention, abuse-prevention, legal, and audit purposes.
Deleted accounts	Eligible personal data is erased or anonymised within approximately 30 to 45 days, subject to legal retention obligations.

16. Your Privacy Rights

Your rights depend on your country, state, province, or region. In general, users may have rights to:

- access personal information held about them;
- receive a copy of personal information, where applicable;
- correct inaccurate or incomplete personal information;
- delete personal information or close an account, subject to legal retention obligations;
- withdraw consent where processing is based on consent;
- object to certain processing, including marketing;
- restrict or limit processing in certain circumstances;
- request data portability where applicable;
- know which categories of third parties receive personal information;
- complain to a data protection authority, privacy commissioner, grievance officer, or other regulator; and
- exercise additional country-specific rights described in the relevant country-specific policy or supplement.

To exercise rights, contact us using the details at the end of this policy. We may need to verify your identity before processing a request. Some information may be retained where required for legal, accounting, security, fraud-prevention, dispute, or compliance reasons.

17. Account Deletion and Data Removal

Users may request account deletion through the app, website, support channel, or any mechanism made available for the relevant app or platform. Account deletion may remove or anonymise account information, learning records, uploaded materials, profile data, and related personal information, subject to lawful retention requirements.

Certain records, such as payment, tax, fraud-prevention, security, complaint, audit, and legal records, may need to be retained for a limited period even after account deletion. Where deletion is requested, we aim to erase or anonymise eligible account data within the period stated in this policy or the applicable country-specific policy.

18. Security Measures

We use reasonable technical, organisational, and administrative measures designed to protect personal information. These may include:

- encryption in transit and, where supported, encryption at rest;
- secure authentication;
- role-based access controls;
- staff and administrator access restrictions;
- cloud security rules and storage access controls;
- app integrity, fraud-prevention, and abuse-prevention checks;
- logging, monitoring, and security review;
- data minimisation and processor restrictions;
- regular review of privacy and security controls;
- breach-response and notification procedures where required by applicable law; and
- confidentiality controls for staff, contractors, processors, and partners.

No digital system is completely secure. However, we take reasonable and proportionate measures to protect personal information against unauthorised access, loss, misuse, alteration, disclosure, or destruction.

19. Changes to this Policy

We may update this Global Privacy Policy from time to time to reflect changes in law, app-store requirements, service providers, technology, product features, payment methods, AI functionality, partner models, or our business operations.

Material changes may be notified through the app, website, email, legal webpage, app-store listing, or other appropriate communication channel. The "Last Updated" date shows when this policy was last revised. Continued use of the Platform after an updated policy becomes effective means the updated policy applies, subject to any consent or re-acceptance requirements under applicable law.

20. Contact Information

Data Controller / Platform Operator: Mathein The Learning Company UK Ltd 25 Strone Park, Dundonald, Belfast, Northern Ireland, BT16 1UW, United Kingdom

Privacy and support contact: privacy@matheinlearning.com support@matheinlearning.com

If the app you use displays a different official support email, you may also use the support contact shown inside that app, on the app-store listing, or on the Mathein legal webpage. Country-specific policies may include additional local contacts, response times, grievance mechanisms, or regulator information.