Scholé

Privacy Policy

https://app.schole.ai/privacy?lang=en

CONTENTS

Summary 1
1. Who we are 2
2. What we collect 2
3. Why we use your data and on what legal basis 3
4. AI, scores and automated decisions 4
5. Who receives your data 5
6. Cookies, analytics and your privacy choices 6
7. Marketing email 7
8. How long we keep your data 7
9. Your rights 8
10. Where your data is processed and how transfers are protected 9
11. Children 10
12. Security 10
13. Additional information for California residents 11
14. Additional information for the United Kingdom 11
15. Additional information for Switzerland 11
16. Additional information for Canada 12
17. Changes to this policy 12
18. Contact 12

Version 2.0, effective 27 September 2026. Previous version: 13 August 2026.

This policy explains how Scholé handles personal data when you use the Scholé learning platform (app.schole.ai, the sites we run for organisations, and guest lesson links) and when we email you. The Olé browser extension has its own privacy notice at /privacy-browser.

Summary

- We store your data in Switzerland. Product analytics and error monitoring run in the EU.
- AI features send your messages to AI providers. Some of them process data in the United States. We tell you who they are and how the transfer is protected.
- We do not sell your personal information, and we do not use your content to train AI models.
- Scores and mastery estimates are there to help you learn. No decision with legal or similarly significant effects on you is made by AI alone.
- You can download your data and delete your account yourself in Settings. For anything else, write to privacy@schole.ai.

1. Who we are

Two companies operate Scholé:

Company	Address	Responsible for
Scholé Sàrl	EPFL, Bâtiment INF, Station 14, 1015 Lausanne, Switzerland	Customers and learners in Switzerland, the European Economic Area (EEA) and the United Kingdom
Scholé Inc.	1209 Orange Street, Wilmington, Delaware 19801, USA	Customers and learners everywhere else, including the United States and Canada

In this policy "Scholé", "we" and "us" mean the company responsible for you under the table above. This is the same split as in our Terms of Service: it follows your country or, if your account comes from an organisation, that organisation's billing country.

If you signed up on your own (with your email address or Google), that company is the controller of your personal data: it decides why and how your data is used.

If your account comes from your employer, school or another organisation (an invitation, a bulk upload, our Integration API, a launch from your organisation's learning system, or an HR system sync), that organisation is the controller of the data it gives us and of your learning data. We process that data on its behalf and on its instructions, under our Data Processing Agreement. This policy still tells you what we do, but your organisation's own privacy notice applies too, and requests about your data should normally go to your organisation. If you send them to us, we pass them on (see section 9).

Contact. For any privacy question or request, write to **privacy@schole.ai**. The same address reaches the people at Scholé who handle data protection. We have no establishment in the EU or the UK.

2. What we collect

Category	Examples	Where it comes from
Account and profile	Name, email address, password (stored as a hash), language, job title, company, department, goals, skills and self-ratings, avatar, optional phone number and date of birth	You, your organisation, or Google when you sign in with Google
Calendar (optional)	When you are busy or free in your Google or Microsoft calendar, as time ranges only, and the study blocks Olé places there; an encrypted token that lets us read and write those blocks	You, when you connect a calendar on your rhythm page; removed when you disconnect; a Google token is also revoked at Google, Microsoft access is removed under My Apps in your Microsoft account
Learning content	Your answers, chat messages, role-play conversations, questions to Olé (our AI assistant), documents you upload, lesson feedback and survey answers	You
Voice	What you say in voice role plays and voice input. The audio is processed in memory to turn it into text and is not stored; the transcript is stored	You
Progress and results	Lessons started and completed, scores, role-play grades and written feedback, mastery estimates, badges and credentials, XP	Generated by the platform from your activity

Category	Examples	Where it comes from
AI-generated information about you	Short summaries of your role and learning progress, recommendations, what the assistant remembers about you	Generated by the platform
Usage and technical data	Clicks and page views inside the platform, device and browser, IP address, error reports	Your browser and our servers
Consent and legal records	Your decisions on cookies, marketing email, the terms and this policy, your age confirmation, with the date and the policy version	You
Billing	Plan, billing email, subscription status, invoices. Card details are entered on Stripe's pages and never reach us	You or your organisation, Stripe
Support	Your messages to support and any screenshot you choose to attach	You
Guest and study sessions	Guest session identifier, IP address, browser, your lesson activity; for research studies, your Prolific participant ID and the version and time of your study consent	You, Prolific
Organisation and sales contacts	Name, email, role and company of people who contact us or who manage a customer account	You or your organisation

We do not ask for sensitive data such as health information, religion or political opinions. Please do not type such information into lessons or conversations. If you do, it is processed like the rest of your learning content.

Google user data. When you connect a Google calendar, Scholé's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. We use that data only to place your study blocks and keep them up to date. We do not use it for advertising, we do not sell it, and we do not use it to train AI models.

3. Why we use your data and on what legal basis

Under the EU and UK GDPR we need a legal basis for each purpose. Swiss law uses similar principles.

Purpose	Legal basis
Creating and running your account, delivering lessons, AI tutoring, role plays, progress tracking and credentials	Contract: we need it to provide the service you or your organisation signed up for
Personalising lessons and recommendations, and estimating your mastery of skills	Contract
Service emails: verification, password resets, assignments, lesson and badge updates, replies to your requests	Contract. You can switch off lesson and progress emails in your profile
Marketing email (learning tips and product news)	Your consent (section 7)
Product analytics with PostHog, including the text of your AI conversations	Your consent through the cookie banner (section 6)

Purpose	Legal basis
Short feedback surveys after some lessons, after the role assessment and, for people who run a school, on the Team mastery page, and matching the answers to the lesson, assessment or school they are about	Legitimate interest in evaluating and improving the training your organisation runs. Answering is always optional
Counting signups without identifying you	Legitimate interest in measuring how many people sign up
Error monitoring and security: detecting faults, abuse and attacks	Legitimate interest in keeping the platform secure and reliable
Managing customer and prospect relationships in our CRM	Legitimate interest in running our business with the organisations we work with
Handling support requests	Contract, or our legitimate interest in answering you when you have no account
Billing and accounting	Contract, and legal obligation to keep accounting records
Keeping records of consent, terms acceptance and age confirmation	Legal obligation to be able to prove consent and compliance
Keeping role-play and conversation transcripts, with your identity removed, after you delete your account, for research and product improvement (section 8)	Legitimate interest in improving our lessons and in research, with the identity removal as the safeguard
Research on how people learn, including studies with academic partners, using de-identified data (names, email addresses and other direct identifiers removed) and publishing only anonymised results	Legitimate interest in scientific research, unless you have opted out (section 9). For organisation-managed accounts, only where the organisation's agreement with Scholé allows it
Research studies you join through a study link	Your consent, given on the study's consent page
Guest lessons opened through a link, without an account	Legitimate interest in giving you the trial you asked for
Complying with the law and defending legal claims	Legal obligation, or legitimate interest in defending our rights

Where we rely on legitimate interest, you can object (section 9). Where we rely on consent, you can withdraw it at any time; this does not affect what happened before you withdrew.

4. AI, scores and automated decisions

You are interacting with AI. Lesson conversations, feedback, role-play characters and Olé are produced by AI systems, not by a person. AI output can contain mistakes.

What the platform works out about you. To adapt your learning, the platform evaluates your answers and conversations. This is profiling:

- **Mastery estimates.** For each skill in a course's knowledge graph, the platform keeps a probability estimate of how well you have mastered it, updated from your answers. The estimates are formative: they decide what to practise next and they expire if they are not refreshed.
- **Role-play grades and feedback.** AI grades practice conversations and writes feedback. You see it, and you can try again.
- **Scores and progress** are shown to you and, if your account comes from an organisation, to that organisation's administrators in dashboards and in exports to their own systems.

- **Recommendations and lesson order** suggest what to learn next. You can change them. Mandatory lessons are set by your organisation, not by AI.

No decision by AI alone. Scholé does not take decisions that have legal or similarly significant effects on you based only on automated processing. No score by itself grants, refuses or removes anything of consequence, such as a job, pay or access to the service. If your organisation uses your results, that is its decision, made by its people and under its responsibility.

Ask for a human review. If you think an AI grade, score or piece of feedback about you is wrong, write to privacy@schole.ai or to support. A member of our team reviews it and replies with the outcome. You can also tell us your point of view and contest the result.

Training. We do not use your content to train AI models. Requests we send through OpenRouter can only go to the seven model hosts on our allowlist (section 10), none of which keeps or trains on prompts (zero data retention). Some of our other AI providers keep prompts for a limited time, for example to monitor abuse; the sub-processor page shows what each one publishes.

5. Who receives your data

Service providers (sub-processors). We use service providers to host the platform, run AI features, send email and take payments. They may only use your data to provide their service to us. The full, current list, with each provider's country, region of processing, purpose and transfer safeguard, is at **app.schole.ai/sub-processors**. In short:

What they do	Providers
Hosting, database, file storage, backups	Microsoft Azure, Switzerland
AI models, speech-to-text and text-to-speech	Microsoft Azure OpenAI and Azure AI Foundry; OpenRouter and the seven model hosts on our allowlist (section 10); Groq; OpenAI; Cerebras
Text extraction from documents you upload	Microsoft Azure Document Intelligence, EU (West Europe)
Product analytics and feedback surveys	PostHog, EU (Frankfurt)
Error monitoring	Sentry, EU (Germany)
CRM, marketing and support email	HubSpot, United States
Company email and Google sign-in	Google Workspace
Payments and invoices	Stripe (Ireland), Mercury (United States)
Credentials issued before our own credential system	Certifier, Poland
Source code and issue tracking (incidental data only)	GitHub, United States

We give organisation customers 30 days' notice before we add or replace a sub-processor.

Your organisation. If your account comes from an organisation, its administrators see your progress, scores, mastery and role-play results, and can export them to their own HR or learning systems.

Prolific. If you take part in a research study recruited through Prolific, Prolific receives only your participant ID and whether you completed the study.

Academic research partners. We may share de-identified learning data (names, email addresses and other direct identifiers removed) with academic research partners for the research described in section 3, under a written agreement that limits its use to that research and forbids any attempt to re-identify you. We never share the data of people who have opted out of research, or of organisation-managed accounts whose organisation's agreement with Scholé does not allow it.

Authorities. We disclose personal data to authorities only where the law requires it.

No selling. We do not sell your personal information.

6. Cookies, analytics and your privacy choices

Necessary storage. The platform stores a few items in your browser that it needs to work, such as keeping you signed in, your language and your cookie choice. These do not need your consent.

Analytics only with your consent. On your first visit a banner asks whether you accept analytics. Until you accept, PostHog's analytics script does not load. If you accept:

- PostHog (EU, Frankfurt) receives how you use the platform;
- PostHog also receives the full text of your prompts and of the AI's answers whenever you use an AI feature. This stops as soon as you withdraw consent.

Feedback surveys. We sometimes ask a few optional questions: at the end of some lessons, after you finish the role assessment and, if you run a school, on the Team mastery page. The survey is run by PostHog and loads whatever your choice. With each answer we send identifiers that let us match it to what it is about: the lesson, your role assessment and its result (role and level), and your school. If you accepted analytics, the answer is also linked to your account in PostHog. If you did not, it is not linked to your PostHog profile, but we can still match it to your assessment or lesson, so it is not anonymous. You can skip any survey.

Signup count. When you create an account, we record a signup event in PostHog. Unless you have already accepted analytics, it carries no email address and no identifier that links it to you.

Error monitoring. Sentry (EU, Germany) receives error reports, including technical context such as the request and your IP address, whatever your cookie choice, because we need them to keep the platform secure and working.

Global Privacy Control. If your browser sends a Global Privacy Control (GPC) signal and you have not made a choice yet, we treat it as a refusal of analytics and record it on your account. If you later accept analytics yourself, your own choice applies.

Change your mind at any time. Use **Your Privacy Choices** on the sign-in and signup pages, **Manage cookie preferences** on this page in the app, or the privacy card in Settings. Each opens the choice again.

7. Marketing email

We send learning tips and product news by email only if you have said yes: by ticking the box when you sign up, by turning on "Tips & product news" under Profile, Email notifications, or by answering yes when the app asks you. You can withdraw at any time with the unsubscribe link in any of these emails or with the same switch. Withdrawing does not affect emails about your account and your lessons.

We ask account holders we had not asked before 25 September 2026 once, in the app. If you do not say yes, you receive no marketing email.

8. How long we keep your data

We delete or de-identify data when it is no longer needed. A job runs every day and deletes records older than these periods:

Data	How long we keep it
Account and profile	As long as you have an account. If you delete your account, it is locked at once and erased 30 days later (see below)
Lesson and chat conversation messages	2 years (730 days)
Role-play records while you have an account	As long as you have an account
Role-play records after your account is erased, with your identity removed	2 years (730 days) after the last activity
XP history and recommendation history	2 years (730 days)
Lesson activity events, progress summaries, questions to Olé	1 year (365 days)
AI request records used to generate personalised scenarios	1 year (365 days)
Clicks and page views inside the platform, assessment timing logs, conversation rename and delete log	90 days
Chat before signup, when you started one but did not create an account	7 days
Documents you upload to create a lesson yourself	90 days
Files attached in the authoring console	7 days
Guest role-play records (no account)	2 years (730 days)
Research study participant data (Prolific ID, IP address, browser, study session)	1 year (365 days)
Error reports in Sentry	90 days
Payment records and invoices	10 years, as accounting law requires
Log of administrator actions in organisation accounts	7 years
Consent, terms and age records	As long as you have an account, and afterwards with your identity removed, as proof of compliance
Database backups	35 days

Data	How long we keep it
Calendar connection (encrypted token, the study blocks we placed)	Until you disconnect the calendar or your account is erased. The busy and free time ranges we read are held in a server cache for at most 5 minutes and are never stored in the database

When you delete your account. You can delete your account in Settings. We lock it immediately. For 30 days you can still ask support to cancel the deletion; nothing is deleted during that time. After 30 days we erase your identity: your name, email, username, phone number, date of birth, avatar, employer and job details, the AI summaries about you and the assistant's memory of you are overwritten or emptied, and every other copy of your email address in the platform is rewritten. In the same run we delete your person and events from PostHog, cancel any running Stripe subscription and remove your details from the Stripe customer record, and delete your HubSpot contact and support tickets. If a provider cannot be reached, we retry until it confirms. Survey answers given without analytics consent are not deleted from PostHog, but once your identity is erased they can no longer be linked to you.

What stays after erasure. Your conversation and role-play transcripts are kept with your identity removed, for research and product improvement, and are deleted at the end of the normal 2-year period above. We do not rewrite what you typed inside a transcript, so a detail you wrote into a conversation yourself (for example your own name) stays in it until that deletion. Invoices stay with Stripe and in our accounts for the period required by law. Organisation audit logs and consent records stay with your email address removed.

9. Your rights

Depending on where you live, you have some or all of these rights:

- **Access**: get a copy of your data and information about how we use it.
- **Portability**: receive the data you gave us in a machine-readable format.
- **Correction**: fix inaccurate data. You can edit most of your profile yourself.
- **Deletion**: have your data erased (section 8).
- **Restriction**: ask us to pause processing while a question is resolved.
- **Objection**: object to processing based on legitimate interest, and to marketing at any time.
- **Opt out of research**: stop the use of your data for research at any time, by writing to privacy@schole.ai.
- **Withdraw consent** for analytics, marketing or a research study, at any time.
- **Human review** of an AI grade or score (section 4).
- **Complain** to a data protection authority (see below).

Do it yourself. In Settings you can download your data (**Download my data** gives you a JSON file with everything linked to your account, once every 24 hours), delete your account, change your email preferences and your cookie choice.

Or write to us at privacy@schole.ai. Requests are free. We reply first within 2 business days. We may ask you to write from the email address of your account, so that we do not give your data to someone else. You can use an authorised agent; we then ask for your signed permission and confirm it with you.

If your account comes from an organisation, the organisation decides on most requests. We tell you that we have passed your request on, and we inform the organisation within 5 business days.

How fast we answer and where you can complain:

Where you live	Law	Our answer	Where you can complain
EEA	EU GDPR	Within 1 month; up to 2 more months for complex requests, and we tell you within the first month	The data protection authority of the EU or EEA country where you live, work or where the problem happened
United Kingdom	UK GDPR and Data Protection Act 2018	Within 1 month; up to 2 more months for complex requests	Information Commissioner's Office (ICO), ico.org.uk
Switzerland	Federal Act on Data Protection (FADP)	Within 30 days; if we need longer, we tell you within the 30 days	Federal Data Protection and Information Commissioner (FDPIC), edoeb.admin.ch
California	CCPA as amended by the CPRA	We confirm receipt within 10 business days and answer within 45 days; up to 45 more days if needed, and we tell you	California Attorney General or California Privacy Protection Agency (CPPA)
Canada	PIPEDA	Within 30 days; up to 30 more days in the cases the law allows, and we tell you	Office of the Privacy Commissioner of Canada (OPC), priv.gc.ca
Anywhere else		We apply the EU GDPR standard	Your local authority, if there is one

If we refuse a request, we tell you why and how you can complain.

10. Where your data is processed and how transfers are protected

- **Storage.** Your data is stored in Switzerland, in Microsoft Azure's Switzerland North region, with backup copies in Switzerland.
- **Analytics and error monitoring** run in the EU: PostHog in Frankfurt, Sentry in Germany. Text extraction from uploaded documents runs in the EU (West Europe).
- **AI features.** To answer you, we send your messages and the context the lesson needs (for example your role and goals) to AI providers:
  - Microsoft Azure OpenAI and Azure AI Foundry. Our accounts are in the United States and Switzerland, and most of our models are deployed globally, so a request may be processed in any Azure region in the world, including the United States. Data at rest stays in the account's region.
  - OpenRouter (United States), which may send a request only to the seven model hosts on our allowlist: Cerebras, Groq, SambaNova, Nebius, Microsoft Azure, Google Vertex AI and Amazon Bedrock. Each is headquartered in the United States or the EU and keeps no prompts (zero data retention). They may serve a request from any of their regions: Microsoft, Google and Amazon from regions worldwide, some also from Canada, and Groq also from Saudi Arabia; OpenRouter does not say which region serves a given request.
  - Speech-to-text by Groq and OpenAI, and some text-to-speech by OpenAI, in the United States. Other text-to-speech runs on Microsoft Azure as described above.
- **EU-only AI processing.** We are introducing EU-only processing of AI requests for customers in the EU, Switzerland and the UK. Until it is switched on for your organisation, the paragraph above applies.

- **Other providers in the United States** include HubSpot, Google Workspace, Mercury and GitHub (section 5).

Switzerland and the EU recognise each other's level of data protection, and both recognise the UK. When data goes to the United States or another country without such recognition, we rely on the European Commission's Standard Contractual Clauses, with the UK Addendum for UK data and the Swiss addendum for Swiss data, and on the EU-U.S. Data Privacy Framework (and its UK and Swiss extensions) where a provider is certified. The safeguard for each provider is on the sub-processor page. You can ask for a copy at privacy@schole.ai.

11. Children

Scholé is not intended for anyone under 16. When you create an account, we ask you to confirm that you are 16 or older, and we keep a record of that confirmation, with its date and the version of this policy in force, as evidence that you gave it. If your employer or school created your account, you confirm your age by accepting our Terms, which require you to be 16 or older, the first time you sign in. Organisations that set up accounts through our Integration API cannot create an account for anyone whose date of birth shows they are under 16, and we do not store that date of birth. If you believe someone under 16 has an account, contact privacy@schole.ai.

12. Security

- Data is encrypted in transit (TLS) and at rest.
- The platform runs on a private Kubernetes cluster in Microsoft Azure, behind a web application firewall. The database accepts only private network connections, and public access to file storage is disabled.
- Staff accounts for Google Workspace and GitHub require multi-factor authentication.
- Security logs are kept for 365 days.
- We are certified to ISO/IEC 27001:2022, and our SOC 2 Type 1 audit is complete.
- If a data breach affects you, we notify the authorities and you where the law requires it.

Calendar data (Google and Microsoft). The only calendar credential we keep is a refresh token. It is stored encrypted (Fernet: AES-128 in CBC mode with an HMAC-SHA256 signature) under a dedicated key held in Azure Key Vault, separate from the database, so a copy of the database alone cannot reveal it. Only the service that reads your free and busy times and places your study blocks decrypts the token; staff never see it, not even in the administration console, where only the encrypted value is shown, and it is never written to logs. We request only when you are busy, never event titles, attendees, locations or notes, and those time ranges stay in a short-lived cache (at most 5 minutes) and are never stored. Calendar traffic goes over TLS and through the same web application firewall, private network and staff multi-factor authentication as the rest of the platform. When you disconnect, we remove the study blocks we placed from your calendar, delete the token and revoke it at Google; Microsoft offers no per-app revocation, so remove Scholé under My Apps in your Microsoft account as well. The token is also deleted when your account is erased.

No system is perfectly secure, but we work to protect your data and review our measures regularly.

13. Additional information for California residents

This section applies to Scholé Inc. and California residents, under the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA).

Categories we collect (section 2 has examples): identifiers (name, email, IP address, account ID); customer records (billing email, phone number); commercial information (plan and subscription history); internet or network activity (use of the platform); audio (voice in voice features, not stored); professional or employment information (job title, company, department); inferences (mastery estimates, recommendations, AI summaries); and sensitive personal information limited to your account login (email and password). We collect it from you, your organisation, Google (if you sign in with Google), Prolific (for study participants) and your use of the platform.

Purposes. The purposes in section 3. We use sensitive personal information only to provide the service and keep it secure, not to infer characteristics about you.

Disclosure. We disclose these categories to the service providers in section 5, for the business purposes in section 3, and to your organisation if it provides your account.

No sale. We do not sell your personal information. If any of our analytics counted as "sharing" for cross-context behavioural advertising under the CCPA, turning analytics off opts you out of it. We honour Global Privacy Control signals as that opt-out (section 6), and the **Your Privacy Choices** link lets you opt out at any time.

Retention. Section 8.

Your rights. To know what we collect and disclose, to delete, to correct, and to opt out of sale or sharing. Because we use sensitive personal information only to provide the service and keep it secure, there is no further use of it to limit. Use Settings or write to privacy@schole.ai; section 9 explains verification, authorised agents and response times. We will not discriminate against you for using these rights.

14. Additional information for the United Kingdom

For UK users, "GDPR" in this policy means the UK GDPR and the Data Protection Act 2018. Scholé Sàrl is responsible for you (section 1). Transfers from the UK to countries without UK adequacy regulations use the UK Addendum to the Standard Contractual Clauses (section 10). You can complain to the Information Commissioner's Office (ico.org.uk).

15. Additional information for Switzerland

For Swiss users, Scholé Sàrl in Lausanne is responsible for your data under the Federal Act on Data Protection (FADP). Your data may be disclosed to recipients in the EEA (Germany, Ireland, the Netherlands, Poland), the United Kingdom and the United States, and, for AI requests on globally deployed Azure models, to any country where Microsoft runs Azure OpenAI, and, for AI requests routed through OpenRouter, to the countries its allowlisted hosts serve from (section 10), including Canada and Saudi Arabia. Disclosures to countries the Federal Council does not recognise as adequate, such as the United States, rely on the Standard Contractual Clauses with the Swiss addendum, or on the Swiss-U.S. Data Privacy Framework where a provider is certified. You can complain to the Federal Data Protection and Information Commissioner (edoeb.admin.ch).

16. Additional information for Canada

For Canadian users, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies. Scholé Inc. is accountable for your personal information (section 1); if your account comes from an organisation, that organisation is accountable for the data it gives us. Our privacy contact is privacy@schole.ai. We collect, use and disclose your information for the purposes in section 3, with your consent: by creating an account you agree to the processing needed to provide the service, and we ask separately before analytics, marketing email and research studies. You can withdraw consent at any time, subject to legal or contractual limits.

Your information is stored in Switzerland and processed in Switzerland, the EU and the United States (section 10), where it may be accessible to courts and authorities under local law. Organisations that need their data kept in Canada can choose Canadian data residency as a paid option. You can access and correct your information (section 9) and complain to the Office of the Privacy Commissioner of Canada (priv.gc.ca).

17. Changes to this policy

When we change this policy, we publish the new version here with a new date and version number. When a change matters for how we use your data, we tell you in the app and ask you to review the new version before you continue.

Version	Date	What changed
2.0	27 September 2026	Names the responsible companies; lists every service provider and where data is processed; adds legal bases, AI and profiling, retention periods, rights and complaint authorities per region, Global Privacy Control, opt-in marketing email, the 16+ age confirmation, and sections for California, the UK, Switzerland and Canada
1.0	13 August 2026	Previous version

18. Contact

Email: **privacy@schole.ai**

Post: Scholé Sàrl, EPFL, Bâtiment INF, Station 14, 1015 Lausanne, Switzerland, or, for customers and learners outside Switzerland, the EEA and the United Kingdom, Scholé Inc., 1209 Orange Street, Wilmington, Delaware 19801, USA.

Your privacy choices

Analytics only load if you accept them. You can change your choice at any time. Manage cookie preferences