

Third Space Learning Inc. Data Protection & Privacy Policy (United States)

For school districts contracting with Third Space Learning Inc.

This is our Data Protection and Privacy Policy ("Privacy Policy") that explains who we are, how we process personal data collected through our website (<https://thirdspacelearning.com/us/>) or any other Services that link to this policy (each, a "Service" and collectively, the "Services"), and, if you are the subject of any of the personal data concerned, what rights you have and how to get in touch with us if you need to.

We operate the Services through the following sites:

Main Website: <https://thirdspacelearning.com/us/>

Applications: <https://app.thirdspacelearning.us>

Student Portal: <https://student.thirdspacelearning.us>

Teacher Portal: <https://teacher.thirdspacelearning.us>

Online classroom (Schola): <https://schola.thirdspacelearning.us>

PLEASE READ THE ENTIRE PRIVACY POLICY VERY CAREFULLY. BY USING ANY SERVICE, YOU AGREE TO BE BOUND BY THIS PRIVACY POLICY IN ITS ENTIRETY. THE ONLY EXCEPTION IS IF WE SIGN A CUSTOM STANDARDIZED DISTRICT DATA PROTECTION POLICY OR TEMPLATE NATIONAL DATA PROTECTION AGREEMENT WHICH WILL THEN SUPERCEDE THESE TERMS.

This policy is specific to users in the United States. If you are located outside the United States, please visit our UK privacy policy for more information about our privacy practices for users outside the United States.

Note about Children: As required by applicable law and our Terms of Service, children under the age of 13 in the U.S. may only use our Services with the express prior consent of a parent or legal guardian. If you are a teacher or other school/district official, you must obtain all necessary parental consents before allowing students to use the Services.

WHO WE ARE

We are Third Space Learning Inc. Our contact and other details are set out at the end of this policy. Third Space Learning Inc. is a Delaware registered C-Corp and is a wholly owned subsidiary of Virtual Class Ltd, a UK registered business.

We provide personalized spoken one-on-one AI math tutoring sessions to children via our secure online classroom, together with access to high-quality math teaching resources and up-to-date professional development modules for teachers through our website. We also provide free access to resources, blog posts and articles to teachers and parents via our website and social media platforms. We provide our Services primarily to schools for the benefit of the teachers and children at the schools concerned, but we may also provide them to individual parents/guardians for the benefit of their children.

WHAT PERSONAL DATA WE COLLECT AND PROCESS

We collect and process personal data as follows:

If you are a teacher (or other members of staff) at a school to which we provide Services

We may collect: your individual contact information, including your name, school name and school address, school district name, your e-mail address, your role/job title at the school, a contact telephone number (which may be your personal mobile number should you choose to give it to us); your timetable availability and the user ID we assign you; in order to enable us to communicate with you in relation to the provision of our Services to you or the school that you work for (for example, in relation to the management and administration of the provision of the relevant Services).

We may also collect other personal information relating to you to in the course of the provision of the Services concerned, which may include, for example, information relating to the school grade/age groups you teach, your experience, material that you access via our learning hub and other information relating to you that is included in any communications between us and you or the school district where you work in the course of the provision of our Services.

We may also collect publicly available information about you or information about you we may acquire from service providers or educational information providers.

If you are a teacher or a parent/guardian who accesses free resources

We may collect: your email address, your job title, the state that you are based in, and your age in order to provide you access to the free resources. Free resources are not intended for children under 13 to download. If we become aware that a child under 13 has attempted to download free resources, we will remove their information.

If you are a student or teacher (or other members of staff) at a school to which we provide Services participating in a program or evaluation trial funded, for example, by the government or an education philanthropy or charity

In the event that our service is being provided to you as you are participating in a program or evaluation trial (commissioned and funded, either in full or in part for example by the government or an education philanthropy or charity), you may be required to provide additional personal information to us in accordance with the requirements of that program or trial. You will be provided with information about the additional personal information that will be collected, the purpose of any additional processing and the data that will be shared with the parties involved in the program or trial including any independent assessment experts appointed.

If we provide Services to you as an individual in relation to the children under your care (a parent/guardian)

We may collect your individual contact information (including your name, the user ID we assign to you, your email address and other similar details) to enable us to communicate with you in relation to the provision of Services to you and other personal information relating to you in the course of the provision of the Services concerned.

We will not process any bank account, credit card or other financial details relating to you, as the Services are currently free for end users (paid for by the school district).

We may also process any other information relating to you that is included in any communications between us and you in the course of provision of the Services.

If you are a Child User or Student User to whom we provide our one-on-one online AI math tutoring sessions (or a teacher or a parent of such a child who wishes to know what information we process relating to students to whom we provide tutoring)

Protecting the privacy of young children is especially important to Third Space Learning. For that reason, we created certain features designed to help protect personal information relating to children who are less than 13 years of age or older if required by applicable law ("Child Users"). This also applies to students who are aged over 13 ("Student Users"). For example, we will not use data from Child Users or Student Users for any advertising purposes.

Third Space Learning does not knowingly permit Child Users or Student Users to use our Services without prior, express consent from a parent or legal guardian, except through agreements with schools or districts or as otherwise permitted under the Children's Online Privacy Protection Rule ("COPPA") and the Family Educational Rights and Privacy Act ("FERPA"). If we learn that data of a Child User has been collected on our Services without prior parental consent, then we will take appropriate steps to delete this information. If you are a parent or guardian ("Parent") and discover that your child under the age of 13 (or a higher age if required by applicable law) has a registered account with our Services without your consent, please contact your child's school and contact Third Space Learning to request that we delete that child's Personal Information from our systems.

How does a child use the Services?

Child Users cannot access or use the tutoring Services without first being added by their school or school district. Child Users and Student Users access the Services through either a learning management system that the school already uses or, if the Child or Student User's school does not use such a system, through our website or through a unique url on our secure platform. Third Space Learning obligates school officials (or other authorized individuals) to first obtain any necessary parental consents before permitting children to access or use the Services. For Child Users and Student Users, Third Space Learning relies on the School to provide the consent necessary under the Children's Online Privacy Protection Rule ("COPPA") to collect and use Personal Information. (Note: FTC staff guidance recognizes an exception to this requirement for services operating in schools - the school's decision to use the online service obviates the need for the operator to get individual parental consent for educational use, provided various requirements are met. It is the duty of the School to ensure those requirements are met.)

Voice and audio data from tutoring sessions

Because Skye is a spoken AI math tutor, tutoring sessions involve the processing of student audio. We capture and process the student's spoken responses for one purpose only: to deliver the instructional tutoring session, so that Skye can understand a student's answers and respond to them in real time. We access the device microphone solely for this instructional purpose and only while the student is actively in a tutoring session; we do not use it to monitor the student, their location, their browsing or their device. The audio is converted to text (a transcript) by our speech-to-text sub-processors so that Skye can teach. We use session audio and transcripts only to deliver the tutoring Service, to support and improve it, and to meet our child-safeguarding obligations.

We do not create or use any biometric voiceprints. Our processing of session audio is limited to speech-to-text transcription (understanding the words a student says); we do not perform speaker identification or voice authentication, and we do not generate or retain any voice template or other biometric identifier capable of identifying a student by their voice. No audio or other student data is used to train third-party AI models. Session audio and transcripts are stored in the United States and are retained in line with the Data Classification and Retention Schedule below.

For our free resources, if we are aware that a Child or Student User has provided data in an attempt to access the resources, we will restrict that user's access to the resources and delete any personal data provided.

What data do we collect about Child Users and Student Users?

We may collect information about the Child Users and Student Users necessary to enable us to deliver the sessions to the Child User or Student User, including name, age, gender, academic school grade, educational needs and capabilities, information about any relevant learning needs or other special needs that we may need to take account of in providing the sessions to the Child or Student User. The information about the child will normally be provided by the child's school or parent, except to the extent that the Child User or Student User provides any information during the tutoring session. We limit the amount of information we collect about a Child User and Student User (in addition to the information provided by the Child or Student User's school or parent) to no more than is necessary to deliver the Services.

What children's information is visible to others?

School officials and our AI tutor may access information about their tutees on the tutoring service platform. The tutor cannot share this information outside of normal classroom interaction (e.g. using a tutee's name to address them), and no data is used to train third party AI models. No tutee's profile is made available or visible to the public through Third Space Learning. Tutees cannot view each other's individual Child or Student User profiles.

Skye is built and operated by Third Space Learning and is powered in part by third-party large language model ("LLM") and speech-to-text providers that act as our sub-processors. These providers process session inputs only to generate Skye's responses in real time. Each such provider is contractually prohibited from using student data to train or develop its AI models, and from retaining student data beyond what is needed to deliver the service. We operate a zero data-retention arrangement with our LLM providers, who do not retain student inputs after generating a response. A current list of our sub-processors, including the data they process and their hosting locations, is set out in Appendix A and in our published Sub-processor List.

We may conduct analysis and research using tutee data, but we aggregate and anonymize data before using it for such purposes. We analyze and track standards and performance development across different age groups, geographies and other categories of tutees and no tutee will be identified directly or indirectly from the aggregated data.

A Note about FERPA:

Certain records for Child Users that are collected or maintained by Third Space Learning are subject to FERPA, meaning we only use tutee data for legitimate educational interests, which include providing the Services. FERPA provides parents (or students if over the age of 18) with certain rights with regard to those records.

If you request information about, or a demonstration, or free trial of, our Services

We may collect your individual contact details, including your name, school name, school address, the state that you are based in, your email address, your role/job title at the school, a contact telephone number (which may be your personal mobile number should you choose to give it to us), and your best time to speak in order to arrange a demonstration or free trial. We may also combine this with other information we obtain about the things you are interested in and that are relevant to the Services provided by us (for example, when you use our Services or browse our website and view particular content) in order to help us ensure that any relevant marketing material that we send you is relevant to what you are interested in.

If we wish to send you advertising, marketing or promotional material

When you engage with our Services in any manner identified above, including when you enter your data for free resources, we may collect and use your individual contact details in order to send you direct marketing material in order to advertise, market or promote our Services. We may combine this with other information we obtain about the things you are interested in and that are relevant to the Services provided by us (for example, when you use our Services or browse our website and view particular content) in order to help us ensure that any marketing material that we send you is relevant to what you are interested in.

You can opt out of marketing communications by clicking the unsubscribe link in our emails.

We will not use data of students and users under 18 for marketing purposes and will not send any marketing materials to students and users under 18.

If you provide goods or Services (or you work for someone who supplies goods or Services) to us.

We may collect your individual contact information to enable us, our group companies or other suppliers of ours or our group companies to communicate with you in relation to the provision of goods or Services by you or the person that you work for (for example, in relation to the management and administration of the provision of the relevant goods or Services) and other personal information relating to you to in the course of the provision of the goods or Services concerned. This may include, for example, bank account or other financial details, personal description and photograph, and other information relating to you that is included in any communications between us and you or anyone you work within the course of the provision of the goods or Services.

If we are assessing your suitability or ability to provide goods or Services to us or to any of our group companies

We may collect relevant personal information relating to you to the extent necessary to enable that assessment to take place – for example, if we need to assess or confirm your age, your skills and previous experience, your qualifications or whether there is anything (for example, relating to your past history, your health or your conduct or reputation) that would adversely affect your suitability or

ability to provide the goods or Services concerned. This will be explained to you in more detail at the time we collect the personal data and, where appropriate, will be subject to your prior consent.

If you are invited to, or attend, an event organized or managed by us

We may collect your individual contact and related information (as well as that of anyone who is attending the event with you) as necessary to enable you and any other relevant individuals to be invited to, and to attend, the event and to facilitate your attendance (for example, dietary or special access requirements).

If you register to use or browse our website or social media platforms

We may collect information on your visits to our website or social media platforms, including the resources that you access and use and how you move around different sections of our app, hub or website for analytics purposes to understand how people use our app, hub, or website so that we can make it more intuitive. We may keep a record of the content on our app, website or social media platform that you have accessed, clicked on and used in order to understand what is relevant to your interests based on content that you have looked at. This may involve the use of cookies, which is explained in our cookies policy.

If you apply for a position with us

We may collect personal information in relation to you in connection with any application by you for a position with us. In that case, we will explain in more detail at the time how and for what purposes we intend to process the relevant personal information.

If you respond to or complete a survey we have sent you or published on our website or provided other feedback

In responding to surveys carried out on our behalf (or to relevant survey invitations), you may disclose information that could make you personally identifiable to the third-party entities carrying out the survey on our behalf or to us. You will, in advance of completing the survey, be told what identifiable information (if any) will be disclosed to us. We may use feedback you have given us from customer experience surveys (Google Forms for example) to help resolve issues or problems that you may be having to improve the service we deliver to you and to improve the service generally. For more detailed information concerning the protection of privacy when responding to surveys or survey invitations, you should contact the entity or individual conducting the survey.

If you provide feedback in surveys or otherwise provide feedback about the Services, we may, with your consent, publish quotes from your feedback along with your name. This information will be publicly available. We will never post personal information about users under 18. If you wish to update or delete your feedback, you can contact us.

DATA WE COLLECT AUTOMATICALLY

Like other websites and online services, we and our analytics providers, vendors and other third-party service providers may automatically collect certain "Usage Information" whenever you access and use the Services. For example, we may collect information regarding how often a user accesses certain features. Usage Information may include the browser and operating system you are using, the URL

that referred you to our Services (if applicable), the search terms you entered into a search engine that led you to our Services (if applicable), all of the areas within our Services that you visit, and the time of day you used the Services, among other information. We may use Usage Information for a variety of purposes, including to select appropriate content to display to you and to enhance or otherwise improve the Services and our products.

In addition, we automatically collect your IP address or other unique identifier ("Device Identifier") for any computer, mobile phone or other device (any, a "Device") you may use to access the Services. A Device Identifier is a number that is automatically assigned to your Device used to access a Service, and our servers identify your Device by its Device Identifier. Some mobile service providers may also provide us or our third-party service providers with information regarding the physical location of the Device used to access a Service, internet service provider (ISP), date and time of your visit, browser language, browser type, referring and exit pages and URLs, amount of time spent on particular pages, which parts of our Services you use, which links you click, search terms, operating system, traffic and related statistics, keywords, and/or other general browsing or usage data.

Usage Information is collected via tracking technologies. For more information about the tracking technologies we use, please review our cookies policy.

Cookies

Like many other websites and apps, we use "cookies" (a small file sent to your computer by a website or device to allow the website or app to store information which uniquely identifies you) or other similar software to collect data in order to assist our users and provide them with a more personal experience. For example, cookies help our systems recognize you if you return to our Services shortly after exiting them. You can disable cookies at your browser or device's settings, but please note that if you do so, some (or all) of the features and functionality of our Services may not be available to you. For more information on opting out of cookies, see our cookie policy available on our website.

We do not use cookies or any other tracking technologies, including web beacons (as discussed below), to direct advertisements to students.

Web Beacons

We may also use web beacons on the Services, in our emails, and in our advertisements on other websites. Web beacons are tiny graphic images that are used to collect information about your visit to the Services, such as the pages you view and the features you use, as well as information about whether you open and/or act upon one of our emails or advertisements. We may also collect the URL of the website you visited immediately before coming to the Services. Web beacons help us analyze our site visitors' behavior and measure the effectiveness of the Services and our advertising. We may work with service providers that help us track, collect and analyze this information.

How We Respond To Do Not Track Signals:

Please note that your browser setting may allow you to automatically transmit a "Do Not Track" (DNT) signal to websites and online service you visit. DNT is a privacy preference that users can set in certain web browsers to inform websites and services that they do not want certain information about their webpage visits collected over time and across websites or online services. However, we do not

recognize or respond to browser-initiated DNT signals, as the internet industry is still working to determine what DNT means, how to comply with DNT, and how to create a common approach to responding to DNT. To find out more about "Do Not Track", please visit <http://www.allaboutdnt.com>.

Global Privacy Control: Although we do not currently respond to browser "Do Not Track" signals, where required by applicable state law (for example, California) we will treat a recognized opt-out preference signal, such as Global Privacy Control (GPC), as a valid request to opt out.

WHAT HAPPENS IF YOU ACCESS THE SERVICES ON A MOBILE DEVICE

If you use the Services through a mobile device, you agree that Third Space Learning may store and use that information for security purposes (for example, for user verification or authentication and to ensure that our APIs are being used appropriately).

WHERE WE STORE YOUR PERSONAL DATA

Where data is stored:

All student data is stored in the United States. The live AI tutoring service is hosted on servers in the United States.

This includes the session audio and transcripts generated during tutoring, which are processed and stored in the United States.

Consent to transfer:

Third Space Learning Inc. is located in the United States. By accessing or using the Services, or otherwise providing information to us, you understand that your information may be subject to processing, transfer, and storage in other locations. In the event that Third Space Learning transfers your Personal Data from the United States to another location, Third Space Learning will ensure that the recipient of your PII offers a level of protection equivalent to that provided in the United States. This may include such measures as entering into standard contractual clauses for the transfer of data, gaining your prior consent, or other appropriate measures in accordance with applicable law.

Where data is processed:

Third Space Learning Inc. is established in the US, with a parent company (Virtual Class Ltd) headquartered in London, UK, and the systems which we use, except as set out below, to process your personal data are hosted in the United States.

In order to provide the tutoring Services, we use a proprietary secure online classroom that we have built and own. All relevant data are processed and stored on that platform in the United States. Our one-on-one math sessions are provided by a proprietary AI tutor called Skye which we control, own, and contain many data security and safeguarding measures. No data is used to train third party AI models.

Where we use third-party sub-processors to help deliver the Services (including the LLM and speech-to-text providers that power Skye, and hosting, logging and data-infrastructure providers),

they process limited personal data only on our instructions and under contract. Our current sub-processors and their hosting locations are listed in Appendix A.

Marketing and sales data collected about schools and school districts are stored in Ireland, a country in the European Economic Area, using Salesforce which is SOC 2 compliant and ISO 27001 certified, and all accounts use two factor authentication alongside other security best practices.

HOW WE SHARE YOUR PERSONAL DATA AND WORK WITH THIRD PARTIES

Where necessary in order to manage our business, we may share relevant personal data with our group companies, service providers (i.e data monitoring or analytic tools) or suppliers, but only to the extent necessary in order to provide the Services concerned. We will only share the minimum amount of personal data necessary for the purpose of processing and, where possible, we will share the personal data in a pseudo-anonymized or anonymized form.

We also may share your Personal Information with third parties with your consent (if permissible under applicable law), as disclosed at the time you provide us with information, and as described below or otherwise in this Privacy Policy:

1. Schools/District Customers

We will share student, teacher, and school employee data with the relevant school/district customer with whom the user is associated. Any such sharing is subject to Third Space Learning's contracts with the relevant school or district. We do not control, and are not responsible for, our customers' handling of your data. If you have questions with respect to data that we process in the context of an agreement or relationship with a school or district, you should direct them to the relevant school or district.

2. Service Providers & Partners

We will share your data with third parties to provide services to us or you in connection with the Services, but subject to confidentiality obligations. For example, we may provide your data to companies that provide services to help us with our business activities or data security, including (without limitation) to providers offering payment processing, hosting, information technology, customer support, and consumer research services. We also work with service providers (eg. Google) to provide us with information regarding traffic on the Services, including the features used when visiting the Services and to provide us with information regarding the use of the Services. We may also work with third party platforms (Eg. Clever SSO) to allow students and school/district officials to access the Services.

A current list of the sub-processors we use to deliver the Services, including the categories of data they process, their processing purpose, hosting location and security certifications, is provided in Appendix A to this policy.

3. Administrative, Legal Reasons, & Academic Integrity Investigations

We may also disclose your data, in response to a subpoena, court order, or when otherwise required by law; in response to bankruptcy proceedings; to defend our rights; in response to a request from law enforcement; to provide information to a claimed owner of intellectual property who claims that

content you have provided to us infringes on their rights; upon request of or as otherwise authorized by an academic institution connected to an investigation into academic integrity; to protect and/or defend any applicable Terms of Service or other policies applicable to the Services; or to protect the personal safety, rights, property or security of any organization or individual. We may also use Device Identifiers, including IP addresses, to identify users, and may do so in cooperation with copyright owners, Internet service providers, wireless service providers or law enforcement agencies, at our discretion. These disclosures may be carried out without your consent or without notice to you.

4. Business Transitions

Third Space Learning may share data with its parent, subsidiaries and affiliates, and investors primarily for business and operational purposes. In the event that Third Space Learning goes through a business transition, such as a merger, acquisition by another company, or sale of all or a portion of its assets, bankruptcy, or other corporate change, including, without limitation, during the course of any due diligence process, your data, will likely be among the assets shared and/or transferred.

Any successor entity will be required to honor the commitments in this policy with respect to personal data, and student personal information will not be sold. Where required by applicable state student-privacy law, student data transferred as part of such a transaction will remain subject to protections at least as protective as those in this policy.

You will be notified via email and/or a prominent notice on Services of any completed change in ownership or uses of your data, as well as any choices you may have regarding your data.

5. Testimonials

We may display personal testimonials of satisfied adult users on our Services in addition to other endorsements. With your consent, we may post your testimonial along with your name. If you wish to update or delete your testimonial, you can contact us.

6. Reference Schools

We may share your school or district name with prospective school, district, or state partners for the purpose of helping them to speak to local schools using Third Space Learning to hear of their experience. We will not share your name or contact details without first contacting you to ask if you are happy to speak with the school.

No Third-Party Advertising

Third Space Learning will never share any data with third parties to allow those third parties to advertise or market to users. We will not mine student data for any purposes other than those agreed to by Third Space Learning's relevant school or district customer. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited. Further, we will not provide targeted advertising to any students through the platform.

Third-Party Content, Links to Other Sites, and Third Space Learning Content Found Outside of the Services

Certain content provided through the Services may be hosted and served by third parties. In addition, the Services may link to third-party websites or content over which Third Space Learning has no control and which are governed by the privacy policies and business practices of those third parties.

Please also note that Third Space Learning content may be included on web pages and websites that are not associated with us and over which we have no control. These third parties may independently collect data. Third Space Learning is not responsible or liable for the privacy practices or business practices of any third party. If you do find our content on third party websites, we will happily answer any queries as to whether it is legitimate, or we may issue the offending sites with DCMA copyright takedown notices.

SECURITY OF YOUR PERSONAL DATA

All personal data processed by us is stored securely (the level of security being commercially reasonable based on the nature of the data concerned and the other relevant circumstances). We use a range of organizational and technical security measures to protect your information to ensure it is not accidentally lost, or used or accessed in an unauthorized way.

Where we have given you (or where you have chosen) a password, you are responsible for keeping this password confidential. We ask you not to share a password with anyone and to use a password that is appropriate (i.e. a mixture of upper and lower case letters, and characters, which isn't used on other sites and isn't easily guessed). Schools are responsible for setting up staff members and granting them access to the platform. It is the responsibility of the school to ensure that only authorized persons have access to personal data. Once a teacher leaves the school or ceases to be involved in the Service, the school should remove access to the Service. We cannot be responsible for unauthorized access caused by the failure of a school to remove a teacher's access.

Unfortunately, no method of transmission of information via the internet is completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our website and any transmission is at your own risk. Once we have received your information, we will use commercially reasonable procedures and security features to try to prevent unauthorized access.

DATA BREACH NOTIFICATION

We maintain procedures to detect, respond to and remediate security incidents affecting personal data. If we become aware of a breach of security that compromises the personal data of students, teachers or other users, we will notify the affected school or district without undue delay and, where a signed district agreement or applicable state law specifies a timeframe (for example, within seven (7) calendar days under New York Education Law §2-d, or within any shorter period required by a signed district agreement), within that timeframe. Our standard notification timeline is within 72 hours and without undue delay. Our notice will describe, to the extent known, the nature of the incident, the data involved, and the steps we are taking in response. We will cooperate with the school or district in meeting any further notification obligations they may have.

THE PURPOSES FOR WHICH WE PROCESS PERSONAL DATA

We process personal data only for the purposes described in this policy. In particular, we process personal data to:

- provide and deliver the Services, including math tutoring and free classroom resources;
- set up, administer and support school, district, teacher, parent and student accounts, and communicate with you about the Services;
- operate, secure, maintain and improve the Services, and meet our child-safeguarding obligations;
- carry out our agreements with schools, districts and other customers, and take steps you request before entering into an agreement;
- for the purposes of substantial public interest in the education of students.
- comply with our legal obligations and respond to lawful requests from authorities; and
- process student personal data only at the direction of, and as authorized by, the student's school or district. Consistent with COPPA and FERPA, we rely on the school or district to provide the authorization and any parental consent necessary for students to use the Services, and we use student data only for legitimate educational purposes - never for advertising or to build non-educational profiles of students.

HOW LONG WE KEEP YOUR PERSONAL DATA

We process personal data only for so long as is necessary for the purpose(s) for which it was originally collected, after which it will be deleted or archived except to the extent that it is necessary for us to continue to process it for the purpose of compliance with legal obligations to which we are subject or for another legitimate and lawful purpose. These time periods are different depending upon the category of personal information and the nature of the processing activity.

Upon termination of your account or upon termination of an agreement with a school/school district, you may request we delete any personal information from our live databases. If deletion requested, Third Space Learning will take commercially reasonable steps to delete any personal information from our live databases in a reasonable amount of time not to exceed ninety (90) days. You understand and agree that Third Space Learning may continue to have Personal Information in archive files or similar databases. You further agree that Third Space Learning has no obligation to delete aggregated or de-identified information. Third Space Learning may retain and use aggregated and de-identified information for any purpose consistent with laws and regulations.

Even if your account is closed, information may remain in backup or archive records and we may retain certain data relevant to preventing fraud or future abuse or for legitimate business purposes, such as analysis of aggregated or de-identified data, account recovery or if required by law. All retained data will continue to be subject to the applicable privacy policy for the Service.

Schools are responsible for ensuring data of teachers, employees, and students are deleted when the user is no longer associated with the school. If the contract with a school is terminated and the school

or end user requests deletion of data, user accounts associated with that school will be terminated and data will be deleted from our live databases.

Data Classification and Retention Schedule

The following schedule sets out the categories of personal data we process in connection with the Skye tutoring Service, the purpose for which each category is held, and how long it is retained. Where a signed district agreement sets a stricter deletion timeline than a period below, that agreement governs. Last reviewed: June 2026.

Data classification	Data held	Purpose	Retention period	Notes / basis
Student data — Student personal data	Full name of student; school name; scores from TSL check-in and check-out questions; the student's self-reported enjoyment of sessions and any confidence-level improvements they report.	Allocate the student to tutoring sessions, monitor growth and recommend lessons. The AI tutor is not given the student's full name or school.	End of the contract term plus a 60-day post-termination notice period, after which the identifiable data is anonymized and cannot be restored; or earlier on request by the school or district, or as required by the district's data privacy agreement.	COPPA's implementing rule (16 CFR §312.10) requires retaining children's data only as long as reasonably necessary. At end of term the identifiable data is anonymized; de-identified data may be retained for research, efficacy and product-improvement and survives contract termination.
Student data — Session recordings (sensitive personal data)	Digital recordings of the tutoring session.	Let school and district staff oversee sessions; quality control; error tracking; improved support for schools.	End of the contract term plus a 60-day post-termination notice period; or earlier on request by the school or district, or as required by the district's data privacy agreement.	Retained for the contract duration to support oversight, QA, error tracking and efficacy review, then deleted within a 60-day wind-down (SDPC / National Data Privacy Agreement model; 16 CFR §312.10). A signed district agreement specifying earlier deletion governs.
Student data — Session transcripts	Written transcripts of the tutoring session.	Investigate any child-protection concern; support the school; QA and error tracking; let teachers see how their students are doing.	End of the contract term plus a 60-day post-termination notice period, after which identifiable data is anonymized and cannot be restored; or earlier on request, or as required by the district's data privacy agreement.	Anonymized at end of term; the de-identified dataset may be retained for research, efficacy and product-improvement and survives contract termination.
School staff & platform users — School staff personal data	Full name, role, email address and phone number of teacher and staff users.	Provide platform access to schedule and manage sessions, select programs, view reporting and access teaching resources; communications tailored to the user's role.	End of the contract term plus a 60-day post-termination notice period; or earlier on request by the school or district, or as required by the district's data privacy agreement.	Staff may request account deletion at any time, actioned within 60 days.
Purchaser & customer — Purchaser data (commercial)	Name and email of the purchaser.	Answer queries about what was bought and provide copies of invoices, contracts and related records.	7 years.	A school or financial auditor may request a copy of an invoice or contract; these contain purchaser details and form the audit trail.

Purchaser & customer — Customer contact and usage data (no child data)	Contact details and product-usage activity of customers (e.g. resources downloaded, log-in frequency). No information about children is held in this category.	Contact customers about the service and help them get value from it; recognize returning customers to tailor onboarding.	3 years after a person stops being a customer or user (also deleted on request).	A school may ask for a list of staff who have used the service; we may also check whether a new customer has used us before, to personalize onboarding.
--	--	--	--	---

HOW YOU CAN ACCESS AND MANAGE YOUR PERSONAL DATA

You may access and manage your personal data as follows:

- You may request access to the personal data we hold about you.
- You may request that inaccurate personal data that we are processing be corrected. You may be required to contact your school to correct certain information provided by the school.
- In certain circumstances (normally where it is no longer necessary for us to continue to process it), you may be entitled to request that we erase the personal data concerned. You may be required to contact your school to ensure your personal data is no longer associated with their account.
- Where we are processing your personal data for marketing purposes or otherwise based on our legitimate interests, you may in certain circumstances have a right to object to that processing. This may include where we are processing personal data relating to children to whom we provide tutoring Services.
- You have the right to opt out of marketing communications using the unsubscribe button at the bottom of email communications.
- In certain circumstances, you may have a right to request us to restrict our use of your personal information.
- Where we are processing personal data relating to you on the basis of your prior consent to that processing, you may withdraw your consent, after which we shall stop the processing concerned.

To access and manage your data as set forth above you may be able to make changes on your profile when you login. Otherwise, you should contact us as set out below.

If you have a complaint about any processing of your personal data being conducted by us, you can contact us.

YOUR STATE PRIVACY RIGHTS

In addition to the rights described above, students, parents and users in certain US states have specific protections under state student-privacy and consumer-privacy laws. This section summarizes the most significant of these.

New York (Education Law §2-d)

For students, teachers and principals in New York, we comply with New York Education Law §2-d and the related Parents' Bill of Rights for Data Privacy and Security. In particular: a student's personally identifiable information will not be sold or released for any commercial or marketing purpose; personally identifiable information is encrypted in transit and at rest; we will not retain student data beyond the term of our agreement with the educational agency and will delete or return it on termination as directed; and our staff and any sub-processors with access to student data receive

training on the federal and state laws governing the confidentiality of that data. A signed Parents' Bill of Rights is included with each New York district agreement.

California (SOPIPA and CPRA)

For California users, we comply with the Student Online Personal Information Protection Act (SOPIPA): we do not use covered student information to engage in targeted advertising, do not build a non-educational profile of a student, and do not sell student information. California residents also have rights under the California Consumer Privacy Act (as amended by the CPRA), including rights to know, delete, correct and opt out of the "sale" or "sharing" of personal information; we do not sell or share student personal information. We honor recognized opt-out preference signals such as Global Privacy Control as described above.

Colorado (Student Data Transparency and Security Act)

For students in Colorado, we act as a "School Service Contract Provider" under the Colorado Student Data Transparency and Security Act (C.R.S. §22-16-101 et seq.). We maintain a comprehensive information security program with administrative, technical and physical safeguards for student personally identifiable information; we do not sell student PII or use it for targeted advertising or to create student profiles for non-educational purposes; we delete student PII when requested by the public education entity or on termination of our agreement; and we will give the contracting school or district clear notice before making material changes to this policy and will notify them as soon as possible of any unauthorized release or misuse of student PII.

Illinois (SOPPA and BIPA)

For students in Illinois, we comply with the Student Online Personal Protection Act (SOPPA): we maintain reasonable security procedures, do not sell or rent covered student information, do not use it for targeted advertising, and enter into a SOPPA data privacy agreement with each Illinois district that lists the data elements we collect and the sub-processors we use. We will notify the school of any breach of covered student information within the timeframe required by SOPPA so that the school can meet its own notification duties. Separately, under the Illinois Biometric Information Privacy Act (BIPA), which regulates "voiceprints" and other biometric identifiers, we do not create or use biometric voiceprints from session audio; were we ever to do so, we would first provide the notice and obtain the written consent BIPA requires.

North Carolina (Student Online Privacy Protection)

For students in North Carolina, we comply with the State's student online privacy protections (N.C. Gen. Stat. §§115C-401.2 and 115C-402.5). We do not sell student information, use it for targeted advertising, or build a profile of a student for non-educational purposes; we maintain a data security plan with access controls; we delete student information on request or at the end of our agreement; and our contracts with North Carolina public school units include the privacy, security and breach-notification provisions those statutes require, including, where applicable, the North Carolina Department of Public Instruction Data Confidentiality and Security Agreement. We do not collect biometric information about students.

Texas (Student Privacy Act and CUBI)

For students in Texas, we comply with the Texas Student Privacy Act (Texas Education Code §§32.151–32.156): we do not sell covered student information, use it for targeted advertising, or build a non-educational profile of a student, and where required we use the unique identifier issued by the Texas Student Data System to mask personally identifiable student information. Texas also regulates biometric identifiers, including "voiceprints," under the Capture or Use of Biometric Identifier Act (Texas Business & Commerce Code §503.001). We do not capture or use biometric voiceprints from session audio; were we ever to do so, we would obtain the consent that statute requires and destroy the identifier within the period it specifies.

Ohio (Senate Bill 29 Protecting Ohio's Children's Information Act)

For students in Ohio, we comply with Ohio's student data privacy requirements, including Senate Bill 29 (the Protecting Ohio's Children's Information Act; O.R.C. §§3319.325–3319.327) and the Ohio Student Records Privacy Act (O.R.C. §3319.321). Educational records remain the property of and under the control of the school district; we use student data only to provide the contracted Services; and we do not sell student data or use it for targeted advertising. Where Skye uses the microphone of a student's school-issued device, it does so solely for the noncommercial educational purpose of delivering the instructional tutoring session, with the school's authorization, and only while the student is actively in a session. We do not access or monitor the location, audio or visual recording features, browsing or other device activity of a school-issued device for any monitoring purpose. We support districts in providing the annual notice to parents of third-party providers that Ohio requires.

Arkansas (Student Online Personal Information Protection Act and Student Data Vendor Security Act)

For students in Arkansas, we comply with the Arkansas Student Online Personal Information Protection Act (Ark. Code §6-18-109) and the Student Data Vendor Security Act (Ark. Code §6-18-2604 et seq.): we maintain reasonable security procedures, do not sell covered student information or use it for targeted advertising or non-educational profiling, and include the privacy and security provisions Arkansas requires in our contracts with local education agencies. We support districts in maintaining the lists of school-service providers that Arkansas requires them to update at the start and midpoint of each school year.

Connecticut (Student Data Privacy Act)

For students in Connecticut, we comply with the Connecticut Student Data Privacy Act (Conn. Gen. Stat. §§10-234aa to 10-234dd). We maintain security procedures consistent with the standards that Act references; we do not sell student information or use it for targeted advertising; student records and student-generated content remain the property of the student or their parent or guardian; and, on discovery of a breach of security involving student information, we will notify the contracting board of education without unreasonable delay and no later than thirty (30) days after discovery.

Users in other states with student-privacy or consumer-privacy laws are afforded equivalent protections under those laws; contact us using the details below for state-specific information.

CONTACTING US

Our contact details are:

Third Space Learning Inc.

3 Gerday Dr, Unit 4 #2810, Wilmington, DE 19804

Contact: Company Secretary

Email: secretary@thirdspacelearning.com or hello@thirdspacelearning.com

Phone: 929-298-4593

UPDATES TO THIS POLICY

We may update our privacy policy from time to time and any changes we make to our privacy policy in the future will be posted on our website. If we make any material changes we will notify you by email (sent to the email addresses we hold on your account) prior to the change becoming effective. Please check back frequently to see if there have been any updates or changes to our Privacy Policy. Your continued use of the Services following an update to this Privacy Policy will constitute your acceptance of the updated Privacy Policy.

We review this policy at least annually, and we maintain an effective date below together.

DATE OF THIS POLICY

This policy was last updated on June 26, 2026

APPENDIX A - SUB-PROCESSOR LIST

The following third parties process personal data on our behalf to deliver the Services. This summary is maintained alongside our detailed Sub-processor List (Exhibit B), which additionally records each sub-processor's registered address and internal owner. All listed sub-processors hold SOC 2 Type II attestation.

Sub-processor	Purpose	Data processed	Hosting location	SOC 2
Ably	Real-time classroom messaging events (e.g. slide or annotation changes).	Classroom messaging events; no PII or student data.	EU	Yes – Type II
Aiven	Enterprise data bus moving data to the data warehouse.	LLM/session events, which can include transcriptions and session health stats.	us-west-2	Yes – Type II
AWS (EC2, Lambda, RDS, Step Functions, CloudWatch, API Gateway)	Core cloud hosting, compute, database, orchestration and logging.	Most session data, encrypted in transit and at rest.	us-west-2 / USA (multi-region)	Yes – Type II

Amazon Chime	Audio and video for the lesson meeting.	IP-address metadata and potentially student audio (for noise cancellation).	USA (multi-region)	Yes – Type II
Google BigQuery	SQL transformation of raw input into data products.	Platform data processed as part of the AI session (name redacted); session events incl. transcriptions.	USA (multi-region)	Yes – Type II
Mage	Orchestrates SQL transforming data in BigQuery.	AI session events from CloudWatch and Rudderstack.	US	Yes – Type II
LangSmith	LLM tracing and analysis.	AI session traces incl. transcriptions, stored for 14 days.	us-central1 (Iowa)	Yes – Type II
OpenAI	Text-to-speech (TTS) generates Skye's spoken audio from the tutor's text.	Tutor utterances (text) only converted to audio. No student personal information or instructions are sent to the model, and no student data is used to train AI models.	us-west	Yes – Type II
Groq	Hosts open-source LLM for router and sub agents.	Current question, most recent and correct answer, visual aid and a static prompt.	US	Yes – Type II
Cerebras	LLM provider for tutor and router agents.	Instructions (set by TSL) and pupil inputs (text and voice utterances); no student data used to train AI models.	US	Yes – Type II
TogetherAI	LLM provider for tutor and router agents.	Instructions (set by TSL) and pupil inputs (text and voice utterances); no student data used to train AI models.	US	Yes – Type II
FireworksAI	LLM provider for tutor and router agents.	Instructions (set by TSL) and pupil inputs (text and voice utterances); no student data used to train AI models.	US	Yes – Type II
AssemblyAI	Speech-to-text (primary) for tutoring audio.	Session audio converted to text transcripts; no student data used to train AI models.	US	Yes – Type II
Deepgram	Speech-to-text (fallback).	Session audio converted to text transcripts; no student data used to train AI models.	US	Yes – Type II

Data sources and rostering / SSO integrations

Some districts connect us to a rostering or single sign-on provider, such as Clever, so that students and staff can be set up and can sign in to the Services. Where this is used, the data flow is inbound: the district authorizes the provider to share roster information (such as student names, grade levels and class assignments) with us so that we can create accounts and deliver tutoring. These providers are the district's chosen rostering/SSO vendors and act on the district's instructions, not ours. We receive data from them rather than sending student data to them for processing so they are data sources and integration partners rather than our sub-processors. Any data exchanged during sign-in is limited to what is necessary to authenticate the user and establish the account.