SUPERSEDED VERSION

This version (v1.0, effective May 15, 2026) was superseded on November 13, 2026. It is provided for reference only. The current Application Privacy Policy is available at www.classcloud.ai/privacy-policy.

ClassCloud
Application Privacy Policy

EFFECTIVE DATE: MAY 15, 2026
LAST REVISED: MAY 15, 2026

Introduction

At ClassCloud, Inc. ('the company', 'we', or 'us'), we respect your privacy and are committed to protecting it as described in this privacy policy ('Policy' or the 'Privacy Policy'). This policy describes the types of information we may collect from you or that you may provide when you use our products and services, ClassCloud (collectively, the "Services"), and our practices for collecting, using, maintaining, protecting, and disclosing that information. Your use of the Services and any information you provide on the Services are subject to the terms of this Privacy Policy, which is incorporated into and subject to our Terms of Service.

Separately, our marketing website at www.classcloud.ai (the "Marketing Site") is governed by a Marketing Website Privacy Policy available at www.classcloud.ai/marketing-privacy-policy. That policy describes how we handle information collected from visitors to the Marketing Site, including through contact and demo-request forms, analytics, and advertising cookies. This Policy applies to the authenticated Services; the Marketing Website Privacy Policy applies to the Marketing Site. Where the two appear to conflict with respect to a specific surface, the policy applicable to that surface controls.

Data Collection

- **Personal Information Collection.** For purposes of this Privacy Policy, "Personal Information" means information that identifies, relates to, or could reasonably be linked with or describes an individual or household, either directly or indirectly. "Personal Information" in this Policy has the same meaning as "Personal Data" in the Data Processing Addendum. "Customer Data" means all data, including Personal Information, that a customer or its authorized users submit to or generate through the Services, excluding metadata, de-identified or aggregated data, and usage analytics generated by ClassCloud's operation of the Services. "Customer Data" in this Policy corresponds to "Subscriber Data" as defined in the Master Services Agreement. We collect Personal Information you provide to us, as well as Personal Information collected automatically and from third-party sources as described below.
- **Our Role as Data Processor.** When ClassCloud processes Personal Information on behalf of a school district customer in connection with the Services, ClassCloud acts as the data processor and the school district is the data controller. ClassCloud processes Personal Information only in accordance with the school district's documented instructions (including the Master Services

Agreement, the Data Processing Addendum, the applicable Service Order, configuration choices made by the district in the ClassCloud administrative console, and any express written instructions the district provides to ClassCloud) and as permitted under applicable Privacy Laws. When you submit Personal Information to ClassCloud outside of a school-district customer relationship (for example, through a sales inquiry, job application, or marketing form on our website), ClassCloud acts as the controller of that Personal Information.

- **Third Parties.** We do not allow third parties to automatically collect Personal Information for their own purposes. Aggregated or combined information, representing a non-identifying summary of data, is treated with the same level of confidentiality and protection as personally identifiable information (PII) on our platform. Our product includes features that allow users to create content within the product or upload content to it. We may request additional details to verify users' identities on our platform. User information does not have to be shared or disclosed to participate in social interactions. All user social interactions through the product are logged, including private and direct messages, for review or audit. Personal Information is processed and stored within the United States, and we do not transfer Personal Information outside the United States without the school district's prior written consent. Where we receive Personal Information from third-party sources at the direction of a school district (for example, through a school information system or identity provider integration), we combine it with Personal Information you provide to us solely to deliver the Services as authorized by the district.

Personal Information That We Collect

Personal Identifiers

- **Types We Collect**: User ID, name, username, district/tenant ID, role (student, teacher, parent, staff), grade level (for students)
- **Source**: From you and from your school district
- **Purpose For Collection**: Account management; app functionality; security and compliance

Contact Data

- **Types We Collect**: Email address, phone number (where provided for SMS notifications), mailing address (for sales/job applicants only)
- **Source**: From you
- **Purpose For Collection**: Account management; transactional and notification communications; first-party marketing (where applicable)

Authentication & SSO Data

- **Types We Collect**: SSO subject identifier, IdP-supplied attributes (name, email, profile picture, group membership), directory synchronization metadata, authentication tokens, login timestamps
- **Source**: From you and from your district's identity provider (e.g., Google, Microsoft, WorkOS-mediated SAML/OIDC)
- **Purpose For Collection**: Account management; security and compliance; app functionality

Student Data & Education Records

- **Types We Collect**: Roster data, class and section enrollment, teacher-student associations, SIS-supplied identifiers, assignment and coursework content where applicable
- **Source**: From your school district (via SIS integration)
- **Purpose For Collection**: App functionality (provision of the Services to the district); product personalization

User-Generated Content & Communications

- **Types We Collect**: Content users create or upload to the platform, chat messages (including private and direct messages), social interactions, comments
- **Source**: From you
- **Purpose For Collection**: App functionality; analytics; security and compliance (including moderation and audit logging)

AI Prompt Content & Outputs

- **Types We Collect**: Prompts, queries, files, and other inputs submitted to AI features; AI-generated text and image outputs returned to the user
- **Source**: From you
- **Purpose For Collection**: App functionality (delivery of AI chat features); product personalization

Usage Data

- **Types We Collect**: Product interactions and behavioral data, in-app search history, feature usage events, page views, session metadata
- **Source**: Collected automatically
- **Purpose For Collection**: Account management; analytics; app functionality; product personalization; security and compliance

Device & Technical Data

- **Types We Collect**: IP address, browser type and version, operating system, device identifiers, request metadata, error reports and stack traces, approximate location derived from IP
- **Source**: Collected automatically
- **Purpose For Collection**: Security and compliance; analytics; app functionality (diagnostics and error resolution)

Sensitive Data

- **Types We Collect**: Categories of sensitive personal information as defined under applicable state privacy laws are not intentionally collected. To the extent users voluntarily submit such information through user-generated content or AI prompts, it is processed only with opt-in consent and subject to the limits described in §6.4 and §10.8.
- **Source**: From you (only if voluntarily provided)

- **Purpose For Collection**: App functionality only; not used for any secondary purpose

Support & Inquiry Data

- **Types We Collect**: Contact information and content of support messages; sales inquiry submissions; job application materials (resume, cover letter, contact details)
- **Source**: From you
- **Purpose For Collection**: Responding to your inquiry; recruiting and hiring (for job applicants); account management

How We Use Your Data

Data collected by the product is limited to the purpose of providing the service, and is limited in use to the purposes outlined in this privacy policy or as otherwise described at the time we collect it.

Data collected by the product is used for the following purposes:

- **First-party Marketing.** We may send marketing emails and other communications about ClassCloud products, services, updates, and events to district administrators, educators, and prospect contacts who have provided their contact information through our sales or marketing channels. We do not send marketing communications to students or use Student Data for marketing purposes. Recipients can unsubscribe at any time using the link in any marketing email or by emailing privacy@classcloud.ai.
- **Third-party Marketing.** We do not use your information for the purposes of tracking and displaying targeted advertising (also known as interest-based or cross-context behavioral advertising) on other websites. You can choose to opt-out of or unsubscribe from first-party marketing or third-party marketing.
- **Account Management.** User data may be processed to facilitate account management, including authentication, profile maintenance, password recovery, and the secure administration of user accounts. Personal Information that we collect will be deleted when it is no longer necessary to provide you with our services. Upon termination or expiration of the underlying customer agreement, or upon a customer's written request, ClassCloud provides the customer with the ability to export Personal Information in a commonly used, machine-readable format for sixty (60) days, after which we securely delete all Personal Information from our systems and those of our subprocessors and will provide written certification of deletion upon request. We may retain Personal Information beyond that period to the extent required by applicable law or necessary to establish, exercise, or defend legal claims. Anonymized data, which is no longer attached to you personally, may be retained for longer periods of time.
- **Analytics.** We use collected data to analyze trends, track user engagement, and improve the performance and functionality of our services. This helps us understand how users interact with our platform and identify areas for enhancement.
- **Application and Platform Functionality.** User data may be processed to support the proper functioning and performance of the application, including authentication, feature delivery, and maintaining the Service's stability and security. We may, from time to time, review, screen, or monitor user-created content. We take reasonable measures to delete all Personal Information from a user's

postings before they are made publicly visible. We moderate interactions between users of the product.

- **Product Personalization.** User data may be processed to personalize the Service, enabling adjustments to features, interface, and functionality in accordance with individual user preferences.
- **Developer Notifications.** User data may be processed to deliver notifications to developers, including updates, alerts, and service-related communications, to support the effective operation and management of applications.

How We Share Your Personal Information

- **Categories of Recipients.**This section describes how and for what purpose we disclose or share your data with third parties. We share data with the following categories of third parties: business transferees, affiliates, professional advisors, parent or owner organizations, and subsidiaries. Personal Information is not sold, rented, or exchanged with third parties for anything of value.
- **Categories and Purposes Shared.**We share the following categories of information with third-parties: contact data, user content data, diagnostic data, identifier data, usage data, web browser data, sensitive data, personal data. The purposes for sharing information include account management, security and compliance, analytics, app functionality, product personalization. We share data with third-parties for internal analytics, research, and product improvement purposes. ClassCloud does not use Student Data or Personal Information to train, improve, or develop AI models accessible to other customers, and contractually requires its third-party AI service providers to do the same. Where logging is enabled to resolve service issues, AI service providers may retain data for the minimum period necessary, no longer than thirty (30) days.
- **Contractual Limits on Recipients.**Contractual limits are imposed on third-parties regarding the extent to which they can use Personal Information that we may disclose to them. Contractual limits prohibit third parties from re-identifying de-identified information. Third parties with access to information are required to provide the same security protections as the company.
- **Business Transfers.**In the event of a merger, acquisition, or bankruptcy, user information may be transferred to an acquiring third party. Users are notified if their information is transferred to a third party in the event of the company's bankruptcy, merger, or acquisition. User information cannot be deleted before it is transferred to a third party. Third-party successors are contractually required to use the same privacy practices as described in this policy.

All the above categories exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties, excluding aggregators and providers of the Text Message services.

This exclusion applies to every category of recipient and every category and purpose of sharing described in this section, including contact data, affiliates, parent or owner organizations, subsidiaries, professional advisors, and business transferees, and it controls over any other statement in this Policy. Text messaging originator opt-in data and consent includes the mobile numbers and consent records collected through ClassCloud Notifications, described in the ClassCloud Notifications section below.

Below is a list of our data sharing partners, provided for transparency. The current, authoritative list of subprocessors that process Personal Information on our behalf is maintained at

www.classcloud.ai/subprocessors, and material changes are communicated to customer school districts with at least thirty (30) days' prior notice.

Amazon Web Services, Inc.

- **Privacy Policy**: https://aws.amazon.com/privacy/
- **Description**: Cloud infrastructure provider. Hosts the ClassCloud application, databases, and stores Customer Data in US-region AWS facilities.

Anthropic, PBC

- **Privacy Policy**: https://www.anthropic.com/legal/privacy
- **Description**: AI model provider. Processes user prompts to generate AI text responses in the ClassCloud chat interface (Claude). Bound by contractual zero-data-retention terms; does not train models on Customer Data.

Google, LLC

- **Privacy Policy**: https://policies.google.com/privacy
- **Description**: Identity provider. Supports “Sign in with Google” for staff authentication and Google Workspace directory integration where customer districts use Google for identity management.

Mailgun Technologies, Inc.

- **Privacy Policy**: https://www.mailgun.com/legal/privacy-policy/
- **Description**: Transactional email delivery provider. Sends account-related and notification emails (e.g., password resets, account alerts, incident notifications) to authorized users.

OpenAI, LLC

- **Privacy Policy**: https://openai.com/policies/privacy-policy
- **Description**: AI model provider. Processes user prompts to generate AI text and image outputs in the ClassCloud chat interface. Bound by contractual zero-data-retention terms; does not train models on Customer Data.

Perplexity AI, Inc.

- **Privacy Policy**: https://www.perplexity.ai/hub/legal/privacy-policy
- **Description**: Search-augmented AI provider. Processes user queries that require real-time web information retrieval and synthesis. Bound by contractual zero-data-retention terms; does not train models on Customer Data.

Not Just Tickets, Ltd d/b/a Plain

- **Privacy Policy**: https://www.plain.com/legal/privacy-policy
- **Description**: Customer support platform. Receives support inquiries from authorized users, including contact information and the content of support messages, solely to facilitate ClassCloud's response.

PostHog, Inc.

- **Privacy Policy**: https://posthog.com/privacy
- **Description**: Product analytics provider. Receives pseudonymized usage events (feature interactions, page views, session metadata) used to measure and improve product performance.

Functional Software, Inc d/b/a Sentry

- **Privacy Policy**: https://sentry.io/privacy/
- **Description**: Application monitoring and error-tracking provider. Receives error reports, stack traces, and limited diagnostic context (e.g., user ID, browser, request metadata) when application errors occur, used solely to diagnose and resolve issues.

WorkOS, Inc.

- **Privacy Policy**: https://workos.com/legal/privacy
- **Description**: Enterprise identity and Single Sign-On (SSO) provider. Facilitates SAML/OIDC sign-in and directory synchronization between school district identity systems and the ClassCloud application.

Groq, Inc.

- **Privacy Policy**: https://groq.com/privacy-policy
- **Description**: AI model provider. Processes user prompts to generate AI text responses in the ClassCloud chat interface. Bound by contractual zero-data-retention terms; does not train models on Customer Data.

ClassCloud Notifications (Text Messages and Voice Codes)

ClassCloud Notifications is an optional, standalone messaging program operated by ClassCloud. ClassCloud is the brand that sends the program's messages. You can use the program with or without a ClassCloud account, and enrolling is not required to use ClassCloud.

Through the program, ClassCloud sends incident-review alerts to confirmed subscribers; one-time codes that you request to confirm your alerts subscription, re-verify an existing subscription, or redeem an invitation you received by email; and replies to HELP, STOP, and START. Messages are sent from the ClassCloud RCS sender, and codes may also be delivered by automated voice call from +1 888-602-5683.

For this program we collect and process your mobile number, which we store encrypted, look up using a keyed hash, and display only in masked form; records of your consent, including the consent text and version you agreed to, the time, and the channel; a hashed version of your IP address and your browser user agent at the time you opt in; delivery status logs for messages and voice calls; verification codes, which we store only as keyed hashes; references to, and statuses of, the incident records an alert concerns; for invitations, the invitation reference, a masked contact, and the invitation status; and the result of an automated bot-protection check.

We use this information only to operate the program: to confirm that you asked to enroll, to send the alerts and codes you request, to respond to HELP, STOP, and START replies, to keep a record of your

consent, to protect sign-up from automated abuse, and to monitor delivery. We do not use your mobile number or consent records for marketing or advertising, and we do not send marketing messages through this program.

Mobile opt-in data and consent collected through ClassCloud Notifications will not be shared with any third parties, including affiliates, parent or owner organizations, subsidiaries, professional advisors, business transferees, or marketing partners, excluding the aggregators and providers of the Text Message services described in the next paragraph, which receive this information only to deliver, host, and secure the program. This information is never sold, rented, or exchanged for anything of value.

ClassCloud uses the following service providers for this program. Twilio delivers text messages and automated voice calls and reports their delivery status. Cloudflare hosts the program, stores its database, provides bot protection (Turnstile), and supports real-time status updates. In this program, these providers' role is limited to delivering, hosting, and securing messaging; it does not include ClassCloud's AI features, and they are separate from the AI model providers listed above.

Statements elsewhere in this Policy about where Personal Information is stored or processed, about encryption or other security measures for Personal Information, and about certifications or audits such as SOC 2 describe the ClassCloud platform and do not describe ClassCloud Notifications. For this program, the safeguards are the ones described in this section: in the program's database, mobile numbers are stored encrypted and looked up by keyed hash, verification codes are stored only as keyed hashes, and IP addresses are stored only in hashed form; the program's pages show mobile numbers only in masked form; and the program's administrative pages require an authorized ClassCloud sign-in. Program information is hosted on Cloudflare's network and delivered through Twilio, and may be processed in the locations where those providers operate. This paragraph does not change any notice or other obligation ClassCloud owes a school district under its agreement.

When you enroll in ClassCloud Notifications, you provide your mobile number and consent directly to ClassCloud, and ClassCloud acts as the controller of that information for this program. If any other part of this Policy conflicts with this section, including the Our Role as Data Processor statement, the Contact Data purposes, the How We Share Your Personal Information section, and the Account Creation and Third-Party Sharing statements, this section controls for ClassCloud Notifications. Enrolling does not change how your school district's data is handled under its agreement with ClassCloud.

You can stop messages at any time by replying STOP (or STOPALL, UNSUBSCRIBE, CANCEL, END, QUIT, REVOKE, or OPTOUT), resubscribe by replying START, and get help by replying HELP or by calling ClassCloud 24/7 Support at +1 888-602-5683. Message and data rates may apply. To make a privacy request about this program, email privacy@classcloud.ai. The ClassCloud Notifications Program Terms in our Terms of Service also apply to the program.

Your Choices

You have certain choices regarding how your Personal Information is collected, used, and shared. This section explains the options available to you and how you can manage your privacy preferences.

- **Account Creation.**To use our Services, you are required to create an account. During account creation, we will collect certain information to establish and manage your account effectively. This information may include, but is not limited to, your name, email address, and a password of your choice. Your account allows you to personalize your experience, track your activities, and access

additional features. We are committed to protecting the privacy and security of your account information in accordance with this privacy policy.

- **Third-Party Sharing.**Users have the ability to share their data with third parties, and such sharing occurs only with opt-in consent. Users can opt out of having their data shared with third parties.
- **Targeted Advertising.** The Services do not engage in targeted, interest-based, or cross-context behavioral advertising, and do not 'share' Personal Information for cross-context behavioral advertising as that term is defined under the CCPA. If you visit the ClassCloud marketing website (www.classcloud.ai), separate disclosures and opt-out controls apply and are described in our Marketing Website Privacy Policy.
- **Access Controls and Sensitive Data.**We understand the importance of safeguarding your data, and therefore, we provide methods to control and restrict access to it. Our platform includes access control mechanisms that allow you to define and manage permissions for your data. Users can interact with trusted users. Users cannot interact with untrusted users, including strangers and/or adults. Users can manage how their data is displayed or shared with others through account settings and privacy controls. These tools enable users to adjust preferences and determine the visibility of certain information. We require a user's opt-in consent before collecting and processing sensitive data. The definition of sensitive data varies based on jurisdiction. Learn more about this in Your Privacy Rights. At any time, users can choose to opt out or stop their sensitive data from being processed. The product offers controls that let users limit how sensitive data is processed. Users must opt in to participate in third-party marketing. Users must opt in to participate in first-party marketing.

Other Sites and Services

- **Third-Party Links and Embedded Content.**The Service may contain links to websites, mobile applications, and other online services operated by third parties. These links are not an endorsement of, or representation that we are affiliated with, any third party. In addition, our content may be included on web pages, in mobile applications, or in other online services that are not associated with us. We do not control websites, mobile applications, or online services operated by third parties, and we are not responsible for their actions.
- **Third-Party Login.**Third-party login is supported for authentication into the Services. When you choose to log in to our services using third-party authentication, such as through social media accounts or other external identity providers, we collect certain information from your chosen third-party platform. This may include basic profile details, such as your name, email address, and profile picture. By opting for third-party login, you grant us permission to access and use this information to create and manage your account and enhance your overall experience with our services. We may also request additional permissions during the authentication process, depending on the third-party provider's requirements. If user information is shared with a third party, it is or would be shared in an anonymous or de-identified format.

Security

We use reasonable, industry-standard practices to protect your Personal Information. Our technical and organizational measures include AES-256 encryption at rest for all Personal Information, TLS 1.3 (or

higher) encryption in transit, role-based access controls under the principle of least privilege, multi-factor authentication for administrative accounts, vulnerability assessments and penetration testing, and 24/7 security monitoring and audit logging. ClassCloud maintains SOC 2 Type II certification, and additional security measures are described in Exhibit A to our Data Processing Addendum. If we become aware of a confirmed unauthorized access, use, disclosure, or destruction of Personal Information under our control, we will notify the affected school district without unreasonable delay and in any event within seventy-two (72) hours.

Cookies

- **In-Product Cookies.** The Services use only cookies and similar technologies that are strictly necessary to operate the authenticated application: authentication and session cookies that keep users signed in to their district's instance of ClassCloud and prevent unauthorized session reuse; security cookies, including CSRF tokens, that protect against cross-site request forgery; and preference cookies that remember user-interface choices (such as theme or sidebar state) within the application.
- **No Advertising or Cross-Site Tracking in the Product.** The Services do not set advertising cookies, retargeting pixels, or cross-context behavioral advertising trackers, and do not use third-party analytics cookies that identify individual users. Product analytics are collected through pseudonymized usage events as described in the Personal Information We Collect table above and in theSubprocessorssection.
- **Marketing Website Cookies.** The ClassCloud marketing website (www.classcloud.ai) uses a separate set of cookies, including analytics and advertising cookies, governed by a separate disclosure in our Marketing Website Privacy Policy. Visitors to the marketing website can manage those cookies through the consent banner displayed on that site.

Your Privacy Rights

- **Scope.** Except as otherwise provided, this section applies to residents of states with privacy laws applicable to us that grant their residents the rights described below.
- **Definition of Personal Information.**For purposes of this section, “personal information” has the meaning given to “personal data”, “personal information,” or similar terms under the applicable privacy laws of the state in which you reside. Please note that not all rights listed below may be afforded to all users and that if you are not a resident of the relevant states, you may not be able to exercise these rights. In addition, we may not be able to process your request if you do not provide sufficient detail to confirm your identity or to understand and respond to it.
- **Special-Category Notices.** In some cases, we may provide a different privacy notice to certain categories of residents of these states, such as job applicants, in which case that notice will apply with respect to the activities it describes instead of this section.
- **Notice and Consent on Practice Changes.** Notice is provided if the context in which data is collected changes. Consent is obtained if the practices in which data is collected change. You have the right to request details on the personal information that we sold, shared, or disclosed to a third-party for a business purpose.

- **Government Requests, Deletion, and Opt-Out.**Notice is provided in the event the company receives a government or legal request for a user's information. Users can request for their data to be deleted from the product or service. Users can request for confirmation that the company processes their data. Users can opt-out of targeted advertising from the product or service.
- **Internal Access Controls.**We maintain secure processes that allow authorized personnel to access, review, modify, and delete information when appropriate (for example: to fulfill your requests or maintain data accuracy).
- **District-Mediated Rights.** Most personal data processed through the ClassCloud platform is collected on behalf of a customer school district. Under federal student-privacy laws (FERPA, COPPA) and similar state laws, ClassCloud is designated as a school official with legitimate educational interests, under the direct control and supervision of the school district, which holds the direct relationship with the individual and is responsible for fulfilling requests about education records and student data. Users may exercise their privacy rights through any of the following paths:
- **RightsUnder U.S. State Privacy Laws.** If you reside in California, Virginia, Colorado, Connecticut, Utah, Texas, Delaware, or another jurisdiction with a comprehensive consumer privacy law, you may have rights including:
- The right to know what categories of personal information we process and the purposes.
- The right to access and obtain a copy of your personal information.
- The right to correct inaccurate personal information.
- The right to delete personal information, subject to legal exceptions.
- The right to opt out of the “sale” of personal information or “sharing” for cross-context behavioral advertising. ClassCloud does not sell personal information and does not share personal information for cross-context behavioral advertising.
- The right to limit the use of sensitive personal information.
- The right not to be discriminated against for exercising any of these rights.
- **Through Your School District.** If you are a student, parent or legal guardian, teacher, or staff member of a school district that uses ClassCloud, start by contacting your district's records officer, principal, or designated FERPA/privacy administrator to request:
- Access to your personal data or education records
- Correction of inaccurate or incomplete information
- Deletion of your personal data, subject to applicable retention obligations
- Restriction of processing
- A copy of your data in a portable, machine-readable format

The district will route the request to ClassCloud, where applicable, and ClassCloud will assist the district in responding within the time periods required by law. If you contact ClassCloud directly with a rights request involving district-controlled data, we will promptly refer the request to your district and will not act on it directly unless legally required.

- **In-ProductSelf-Service.** Authorized users can manage certain personal data and preferences directly inside ClassCloud:
- Profile information — edit display name, profile picture, and AI context preferences in User Settings.

- Notification preferences — enable, disable, or change the channel (email, SMS) for account alerts and incident notifications in Settings → Notifications.
- SMS opt-out — reply STOP to any ClassCloud text message to immediately unsubscribe.
- Email opt-out — use the “unsubscribe” link in any non-transactional email, or change notification preferences in Settings.
- **Direct Contact with ClassCloud.** If your personal data was collected by ClassCloud as an independent controller (for example, you submitted a sales inquiry through our website, applied for a job, or otherwise interacted with us outside of a school-district customer relationship) you may contact us directly:

ClassCloud, Inc.
Attn: Privacy Officer
169 Madison Avenue
Suite 38560
New York, NY 10016
privacy@classcloud.ai

- **Verification.** Upon receipt of your request, we will initiate the identity verification process to confirm that you are the individual for whom we hold information in our system. This verification procedure necessitates your cooperation in supplying relevant information, allowing us to compare it with the details you previously furnished. Depending on the nature of your request, we may request specific information to align with our existing records, or we may reach out to you using a previously provided communication method (such as phone or email). In certain situations, alternative verification methods may be employed based on the circumstances. We will respond within the time period required by applicable law — typically 45 days under CCPA, VCDPA, CPA, CTDPA, UCPA, TDPSA, and DPDPA, with a single extension where reasonably necessary.
- **Uses.** Any personal information disclosed in your request will solely be utilized for the purpose of confirming your identity or validating your authority to make the request. We will make every effort to minimize the need for additional information for verification purposes. However, if it is impossible to verify your identity using the information in our records, we may request additional details to ensure security and prevent fraud. Any supplementary information you provide for verification will be promptly deleted upon the completion of the verification process.
- **Authorized Agents.** Your authorized agent may be able to make a request on your behalf. However, we may need to verify your authorized agent’s identity and authority to act on your behalf. We may require a copy of a valid power of attorney given to your authorized agent pursuant to applicable law. If you have not provided your agent with such a power of attorney, we may ask you to take additional steps permitted by law to verify that your request is authorized, such as by providing your agent with written and signed permission to exercise your rights on your behalf, the information we request to verify your identity, and confirmation that you have given the authorized agent permission to submit the request.
- **Appeals.** If we deny your rights request in whole or in part, you may appeal the decision by replying to our response or by emailing privacy@classcloud.ai with the subject line “Privacy Rights Appeal.” We will review the appeal and respond within 60 days, or sooner where required by applicable law. If you are dissatisfied with the outcome of the appeal, you may contact your state attorney general.

Children's Privacy Notice

- **User Audience.**ClassCloud is intended for use by K-12 students (including children under 13), teens, teachers, parents, and guardians in a school setting. Because the platform is licensed by school districts rather than by individual families, ClassCloud relies on the school-consent exception under the Children's Online Privacy Protection Act (COPPA): the school provides consent on the parent's behalf for ClassCloud to collect personal information from students under 13 for educational purposes.
- **District Consent Materials.** Before a school district enables ClassCloud for student use, we provide the district with:
- Direct notice describing the Personal Information ClassCloud collects from students, how it is used, and with whom it is shared; and
- A written acknowledgment in which a school representative confirms their authority to consent on behalf of parents and identifies themselves by name and title.
- **District Control of Student Data.** Personal Information collected from students in the course of providing the service to a school district remains under the direct control of the district for purposes of use, retention, and deletion. ClassCloud will honor a parent's request, made through the district, to review or delete the Personal Information ClassCloud holds about their child, except where applicable law requires us to retain it. Districts manage student accounts (including provisioning, role assignment, and deactivation) through the ClassCloud administrative console, and education records are loaded into the platform through the district's standard student-information-system integration.

Changes To This Privacy Policy

- **Direct written notice to the school district customer.** Because ClassCloud operates a B2B service to public and private K-12 educational institutions, our direct customers are the school districts and educational institutions that subscribe to the platform on behalf of their students, parents, and staff. When we make a material change to the Privacy Policy, Master Services Agreement, or Data Processing Addendum (the latter available at www.classcloud.ai/dpa), we provide the customer's primary administrative contact with at least sixty (60) days' prior written notice before the change takes effect, sent by email and other reasonable means.
- **Notice of Consent Changes.**In addition to modifying this Privacy Policy and updating the effective date, we will contact you (either through the product or otherwise) to gain your consent if we change or modify the practices in which data is collected.

How To Contact Us

If you have questions or concerns regarding this Privacy Policy, please contact us using the means described in this section.

A grievance or remedy mechanism is available for users to file a complaint in the event their content or account is restricted or removed. Please use the information below to contact us.

ClassCloud, Inc.
Attn: Privacy Officer

169 Madison Avenue
Suite 38560
New York, NY 10016
privacy@classcloud.ai