# Imagine Learning Privacy Policy Frequently Asked Questions

## Cookies

### What are browser cookies? Can I opt out?

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added, and the cookie helps analyze web traffic or lets you know when you visit a site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes, and dislikes by gathering and remembering information about your preferences.

You may choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the Website.

Imagine Learning's Services do not currently respond to "Do Not Track" signals sent by your browser.

## Security Practices

### What practices does Imagine Learning employ to protect personal data?

In addition to the protections afforded by our cloud hosting providers, practices employed at Imagine Learning to protect personal data include, but are not limited to:

- **Certification**. Imagine Learning's Information Security Management System (ISMS) has been certified as compliant with the ISO/IEC 27001:2013 security standard by a dual-accredited certification body.
- **Data encryption and storage**. Data is encrypted in transit (SSL/TLS) and at rest (SHA 256 or greater). Personal information is stored and processed within the continental United States.
- **Access**. Access to personal information is restricted to a limited number of Imagine Learning employees who need such access to perform their job.
- **Data Systems Monitoring.** Imagine Learning employs several third-party services that continuously monitor and scan our online services for vulnerabilities. Employees dedicated to operating our services monitor these reports and receive automated alerts when performance falls outside of prescribed norms.
- **Incident Response Plan.** Imagine Learning maintains an incident response plan.
- **File Transfer Protocol**. Data is securely transferred to Imagine Learning using Secure File Transfer Protocol (SFTP) or other equivalent authorized secure file transfer services.
- **Firewalls**. Anti-virus software and firewalls are installed and configured to prevent malicious or unauthorized traffic.

- **Security audits**. Imagine Learning conducts security audits and code reviews, both by external and internal providers.
- **Secure programming practices**. Imagine Learning software developers are aware of secure programming practices and strive to avoid introducing errors in our applications (such as those identified by OWASP and SANS) that could lead to security breaches.
- **Employee account protection**. Each user of Imagine Learning is required to create an account with a unique account name and password. Single Sign-On (SSO) users are authenticated with secure tokens.
- **Facility security**. Imagine Learning is located inside the continental United States. Physical access is protected by electronic access devices, with monitored security and fire/smoke alarm systems.
- **Security Breach**. In the event of a security breach that results in unauthorized release of personal data, Imagine Learning will notify affected customers of such breach, will investigate, and will restore the integrity of its data systems as soon as possible. We will fully cooperate and assist with required notices to those individuals affected by such breach.
- **Employee Training**. Imagine Learning has designated privacy and data security officials to oversee employee security training and compliance.

# California Education Code § 49073.1 and SOPIPA Compliance

## What policies and practices does Imagine Learning employ to demonstrate compliance with California Education Code § 49073.1 and SOPIPA?

Technology services agreements entered, amended, or renewed by a California LEA on or after January 1, 2015 must follow specific requirements. These requirements apply to contracts for services that utilize electronic technology, including cloud-based services, for the digital storage, management and retrieval of pupil records, as well as educational software that authorizes a third-party provider to access, store and use pupil records. Imagine Learning complies with these requirements in the following ways:

- *The procedures by which 1) pupils may retain possession and control of their own pupil-generated content; 2) a pupil may transfer pupil-generated content to a personal account; and 3) parents, legal guardians, or eligible pupils may review personal data in the pupil's records and correct erroneous information are outlined as follows:*

  As noted in our Privacy Policy, Imagine Learning promptly routes these requests to the School or Authorized Person with direct control over the PII. The Services are licensed directly to Schools and are accessible only via a sponsoring School, rather than individual or home users. More specifically, a School's site code is required to access the Services. As owners of pupil records, the School or Authorized Person is the first point of contact for students, parents, and legal guardians to review, correct, export, and otherwise control pupil records and pupil-generated content. The School or Authorized Person is in the best position to accurately verify

the identity of the student or the parent/legal guardian. Imagine Learning stands ready to assist the School or Authorized Person as needed.

- *Service Provider shall take actions to ensure the security and confidentiality of pupil records, including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of pupil records, via the following measures:*

  See the **Security Practices** section of this Imagine Learning Privacy Policy FAQ.

- *In the event of an unauthorized disclosure of a pupil's records, Service Provider shall report to an affected parent, legal guardian, or eligible pupil pursuant to the following procedure:*

  The School or Authorized Person is our first point of contact in the event of an unauthorized disclosure. The School or Authorized Person will be notified immediately, including details about the nature of the disclosure and efforts being made to address it. Each School has its own policies and procedures for responding to an unauthorized disclosure of protected information that aligns with its local laws and regulations. Imagine Learning will work in conjunction with the School to determine if, how, and when affected parents/legal guardians or eligible pupils will be notified.

- *Service Provider shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the Services agreement:*

  As noted in our Privacy Policy, Imagine Learning has strict policies about what data is collected, how it is used, and how it is not used.

- *Service Provider certifies that a pupil's records shall not be retained or available to the Service Provider upon completion of the terms of the Services Agreement, except for a case where a pupil chooses to establish or maintain an account with Service Provider for the purpose of storing pupil-generated content, either by retaining possession and control of their own pupil-generated content or by transferring pupil-generated content to a personal account. Such certification will be enforced through the following procedure:*

  As noted in our Privacy Policy, Imagine Learning does not retain students' PII after a relationship with a School is terminated.

- *Service Provider agrees to not disclose, compile, or allow a third party to use, disclose, or compile the personal information of a minor for marketing or advertising specific types of products or services.*

  As noted in our Privacy Policy, Imagine Learning has strict policies about what data is collected, how it is used, and how it is not used.

# New York Ed Law § 2-d Compliance

## What policies and practices does Imagine Learning employ to demonstrate compliance with NY Ed Law § 2-d requirements?

Section 2-d requires that third party contractors:

- *May not sell or use PII for marketing purposes.*

  As noted in our Privacy Policy, we do not sell personal information, nor do we use or disclose the student information we collect for behavioral targeting of advertisements to students.

- *Must enter into a written agreement with a New York education agency where a third party contractor agrees to comply with that agency's parents bill of rights.*

  Imagine Learning is familiar with the typical information in a parents bill of rights and will agree in contract to a New York education agency's parents bill of rights.

- *Must enter into a written agreement that states the following:*

  - *The exclusive purposes for which the student, teacher or principal data will be used;*
  - *How the third party contractor will ensure that subcontractors, persons or entities with access to student, teacher or principal data with, if any, will abide by data protection and security requirements;*
  - *When the agreement expires, and what happens to the student, teacher or principal data upon expiration of the agreement;*
  - *If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and*
  - *Where the student, teacher or principal data will be stored and the applicable security protections, including whether the data will be encrypted.*

  Imagine Learning is familiar with these contractual requirements and will comply with a request by an educational agency.

- *Must provide training to officers or employees who have access to student, teacher or principal data on the federal and state law governing confidentiality of data.*

  Imagine Learning ensures that staff are trained and systems are in place to provide required security and confidentiality of student records.

- *Must limit access to education records to individuals with legitimate educational interests.*

  "We do not collect data for collection's sake, and access is limited and appropriate"

- *Must notify the educational agency of any security breach resulting in an unauthorized release of data by the third party contractor or its assignees… in the most expedient way*

*possible without unreasonable delay.*

Imagine Learning takes prompt corrective action to remedy any security breach, to mitigate to the extent practicable any harmful effect of an unauthorized use or disclosure of protected information, and take any other action required by applicable federal and state laws and regulations pertaining to such security breach. We provide written notice to the district as soon as possible after discovery of a security breach.

# Illinois SOPPA Compliance

## What policies and practices does Imagine Learning employ to demonstrate compliance with Illinois SOPPA requirements?

SOPPA requires that vendors/operators:

- *Must implement and maintain reasonable security practices that otherwise meet or exceed industry practices to protect student information from unauthorized access, destruction, use, moderation, or disclosure.*

  As noted in the **Security Practices** section of this Privacy Policy FAQ, Imagine Learning employs many security practices designed to protect student information.

- *Must enter into written agreements with schools, districts, and boards of education before PII is transferred.*

  Imagine Learning is familiar with the IL-NDPA model contract drafted by the Illinois Data Privacy Alliance. For fastest processing, please send this or other data sharing agreements to contracts@imaginelearning.com.

- *Must notify schools of any breach of students' PII as quickly as possible but absolutely within 30 days of the breach.*

  We agree to and comply with this requirement. Requirements like this are often included in district data sharing agreements, including the IL-NDPA agreement.

- *Must provide schools with a list of any third parties or affiliates to whom the operator is disclosing covered information.*

  This is available and kept up to date in the **Sub-Processors** section of this Privacy Policy FAQ.

- *Must delete, within a reasonable time period, a student's covered information if the school or school district requests deletion of covered information.*

  This is described in our Privacy Policy and SOPPA-compliant data destruction requirements are included in the IL-NDPA agreement.

- *Must publicly disclose material information about its collection, use, and disclosure of covered information, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.*

  Our Privacy Policy meets SOPPA's disclosure requirements.

- 

- *May not engage in targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application.*

  Imagine Learning complies with this requirement. See our Privacy Policy for details.

- *May not use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of K through 12 school purposes.*

  Imagine Learning complies with this requirement. See our Privacy Policy for details.

- *May not sell or rent a student's information, including covered information.*

  Imagine Learning complies with this requirement. See our Privacy Policy for details.

# Sub-processors

## What sub-processors does Imagine Learning use to provide its Services?

Further information about these sub-processors are available at their respective website.

| Sub-processor | Processing Location | Purpose / General Function | Data Shared |
|---|---|---|---|
| Amazon Web Services, Inc. | United States | Data storage | Encrypted personal information |
| Atlassian (StatusPage.io) | United States | Voluntary subscription service for incident communication | User-submitted email or phone number |
| Auth0® | United States | Single Sign-On provider | SSO ID (only shared if authorized by school) |
| Box, Inc. | United States | Secure file sharing | Encrypted personal information |
| Blackboard Inc. | United States | Video Conferencing, Instructional learning | Personal information shared during recorded instruction |
| ClassLink | United States | Single Sign-On provider, rostering | SSO ID (only shared if authorized by school) |
| Clever® | United States | Single Sign-On provider, rostering | SSO ID (only shared if authorized by school) |
| Databricks | United States | Hosted data warehousing and transformation | Encrypted personal information |

| | | | |
|---|---|---|---|
| Educational Testing Service (ETS) | United States | Essay scoring and feedback engine | Anonymous student essay responses |
| Genius SIS | United States | Video Conferencing, Instructional learning, Distance Learning programs | Encrypted personal information |
| Google Marketing Platform (Google Analytics) | United States | Website analytics | Non-identifiable data (e.g., device type, OS, browser type) |
| Google reCAPTCHA | United States | Spam and abuse protection | Behavioral data to distinguish human users from bots for security purposes |
| Hubspot | United States | Customer relationship management (CRM) for sales & marketing | Customer contact information |
| Learnosity Inc. | United States | Assessment tools and analytics | Anonymous assessment data |
| LogRocket | United States | Product analytics | Anonymous product analytics data |
| Microsoft Corporation | United States | Data storage (Microsoft Azure), SQL Server, Email/productivity | Encrypted personal information |
| MetaMetrics® | United States | Lexile assessment tools | Non-identifying usage data for royalties |
| Middlebury Interactive Languages | United States | World language instruction | Encrypted personal information necessary for instruction (i.e., first/last name, student ID, course #, school ID) |
| New Relic | United States | Network traffic monitoring | Anonymous data |
| Oracle Corporation (Eloqua) | United States | Customer contact / communication | Customer contact information (e.g., name, title, email, district) |
| Pendo.io, Inc. | United States | Service usage analytics | Teacher / Administrator username and first/last name, product usage analytics |
| Renaissance Learning | United States | SaaS-based educational software & assessments | Encrypted personal information |
| SingleIntegration | United States | Education technology data integration software | Encrypted personal and student information necessary for rostering |
| Snowflake | United States | Hosted data warehousing and transformation | Encrypted personal information |
| ZenDesk | United States | Helpdesk services | Teacher/Administrator name and contact information |
| Zoom | United States | Video conferencing, Instructional learning | Personal information shared during recorded instruction |

Last updated:  September 13, 2022