

# Imagine Learning

## Privacy Policy

---



Imagine Learning's mission is to teach language and literacy to the children of the world. We are constantly innovating in order to improve the lives of children, and we recognize our moral and legal responsibility to protect student privacy and ensure data security.

This policy outlines Imagine Learning compliance with federal privacy laws and details our data stewardship and security practices.

### COPPA compliance

The primary users of Imagine Learning are young children. The Children's Online Privacy Protection Act (COPPA) protects children under the age of 13. School officials and teachers are authorized under COPPA to provide consent on behalf of parents; therefore, Imagine Learning does not obtain parental consent directly. A teacher or school district official provides consent for a child under the age of 13 to use Imagine Learning when they create an Imagine Learning account for that child.

For more information about COPPA, you may visit [OnGuard Online](#).

### FERPA compliance

The Family Educational Rights and Privacy Act (FERPA) provides parameters for what is permissible when sharing student information. Imagine Learning is authorized by schools and districts under the FERPA "school official" exception to receive and use educational data to provide educational services. This data has significant educational value; apart from enabling the creation of accounts with which students access the Imagine Learning individualized learning path, the data allows teachers to track student growth and identify students who need intervention. This information is used only for academic purposes. We do not collect data for collection's sake, and access is limited and appropriate. See *Data Stewardship* for more information about how we use and protect data we collect.

### Data Stewardship

This section provides information about Imagine Learning data stewardship practices and explains how we collect, use, and maintain student personal information.

### Data collection

When a school or district creates a student account, Imagine Learning begins to collect information about students. Some of the data stored is personally identifiable information (PII).

The following is a list of data fields that are populated to create a student account.

- First name
- Last name
- Grade level
- Language
- Student number
- Student username
- Password
- Organization number
- SSO ID

As students use Imagine Learning, additional data is collected, including assessment scores, curriculum progress, student audio recordings, and student responses to writing prompts.

Imagine Learning also collects some personal information about teachers and administrators when a school or district creates accounts. This data potentially includes first and last name, e-mail address, and school or district name.

## Data use

Data we collect is used to provide educational services. For example, Imagine Learning makes audio recordings of a child reading and speaking. The audio recordings are played back to the child so she hears how she sounds. Teachers listen to the audio files for an accurate and descriptive measure of student progress. These audio recordings dramatically increase student reading and language fluency.

Imagine Learning tracks and assesses a student's development as they progress through the curriculum. This data is used to generate reports that allow teachers to evaluate student progress, identify students who need intervention, and discover students that can be taught together as a group. Imagine Learning does not sell student personal information, nor do we use or disclose the student information we collect for behavioral targeting of advertisements to students.

We retain some de-identified data (data we have made anonymous by removing all personally identifiable information) to conduct statistical research. This research helps us evaluate the effectiveness of Imagine Learning and improve our product.

## Data disclosure and access

Imagine Learning acknowledges the right parents and legal guardians have under FERPA to review any educational data we collect pertaining to their children. Upon request, and after verifying identity, we will provide parents and legal guardians access to this data within 45 days. However, we recommend that parents first contact their child's school.

PII data collected by Imagine Learning is accessible only to a limited number of Imagine Learning employees who need the data to perform their job.

## Data retention and management

Data maintained by Imagine Learning is protected in a secure environment. See *Security Overview* for more information about Imagine Learning security practices.

All PII provided to Imagine Learning will be destroyed upon termination of our relationship with the school or district, or when it is no longer needed for the purpose for which it was provided.

## Data destruction

Imagine Learning employs United States Office of Education best practice recommendations for data destruction.

Imagine Learning uses these processes for data destruction:

- Data is destroyed within 90 days of termination of a relationship with a school or district.
- Data is destroyed using National Institute of Standards and Technology (NIST) clear method sanitization that protects against non-invasive data recovery techniques.
- Sensitive data will not be disposed of using methods (e.g.; file deletion, disk formatting, and one-way encryption) that leaves the majority of data intact and vulnerable to being retrieved.
- The individual who performs the data destruction signs a certification form describing the destruction.
- Occasionally, non-electronic media used within Imagine Learning may contain PII. When these documents are no longer required, the non-electronic media is destroyed in a secure manner (most typically using a shredder) that renders it safe for disposal or recycling.

## Security overview

At Imagine Learning, we are serious about our data stewardship responsibilities. We have implemented several security measures to protect PII from unauthorized disclosure.

### Software security

Imagine Learning has implemented privacy and security practices which are compliant with FERPA and COPPA; however, to achieve comprehensive protection of student PII, it is necessary for each school or district to use secure practices as well.

#### **Data encryption**

Data is encrypted in transit and at rest.

#### **File Transfer Protocol**

Data is securely transferred to Imagine Learning using File Transfer Protocol (FTP) over secure (SSL/TLS) cryptographic protocol.

**Firewalls**

Anti-virus software and firewalls are installed and configured to scan our system. The firewall is periodically updated and configured so users cannot disable the scans.

**Security audits**

Imagine Learning conducts security audits and code reviews, both by outside providers and by executive summary.

**Secure programming practices**

Imagine Learning software developers are aware of secure programming practices and strive to avoid introducing errors in our application (like those identified by OWASP and SANS) that could lead to security breaches.

**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.

**Employee compliance with security procedures**

Imagine Learning has designated a chief security officer to oversee employee security training and compliance. The chief security officer also oversees the storage and destruction of sensitive data.

**Changes to our privacy policies**

Imagine Learning periodically reviews the processes and procedures described in this document to verify that we act in compliance with this policy. If we determine that a change is necessary to improve our privacy practices, we may amend this policy. Changes will be posted 30 days prior to their implementation.

Privacy policy effective: January 1, 2015

Policy last updated: January 23, 2015

**Contact us**

If you have questions or concerns about Imagine Learning privacy practices, you may send an email to [privacy@imaginelearning.com](mailto:privacy@imaginelearning.com).