Privacy Policy

EdTech Games' mission is to revolutionize educational software. 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 EdTech Games compliance with federal privacy laws and details our data stewardship and security practices.

COPPA compliance

The primary users of EdTech Games 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, EdTech Games does not obtain parental consent directly. A teacher or school district official provides consent for a child under the age of 13 to use EdTech Games when they create an EdTech Games 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. EdTech Games 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 EdTech Games 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 EdTech Games 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, EdTech Games 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 EdTech Games, additional data is collected, including assessment scores and curriculum progress.

EdTech Games 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. EdTech Games 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 and identify students who need intervention. EdTech Games 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 EdTech Games and improve our product.

Data disclosure and access

EdTech Games 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 EdTech Games is accessible only to a limited number of EdTech Games employees who need the data to perform their job.

Data retention and management

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

All PII provided to EdTech Games 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

EdTech Games employs United States Office of Education best practice recommendations for data destruction.

EdTech Games 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 is completely removed using *Eraser* rather than methods such as file deletion, disk formatting, and one-way encryption that leave the majority of data intact and vulnerable to being retrieved.
- Occasionally, non-electronic media used within EdTech Games 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 EdTech Games, we are serious about our data stewardship responsibilities. We have implemented several security measures to protect PII from unauthorized disclosure.

Software security

EdTech Games 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 when in transit.

File Transfer Protocol
Data is securely transferred to EdTech Games 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
EdTech Games conducts security audits and code reviews.

Secure programming practices
EdTech Games 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 EdTech Games 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

EdTech Games is located inside the continental United States. Physical access is protected by physical locks and fire/smoke alarm systems.

Changes to our privacy policies

EdTech Games 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: April 25th, 2018