FATHOM READS®

Privacy Policy

Fathom Technologies®, LLC d/b/a Fathom Reads ("Fathom") has developed this privacy policy to inform students, parents, and educators of policies and procedures regarding the collection, use, and disclosure of personally identifiable information and non-personal information we receive from users of our platform www.fathomreads.com and other Fathom websites where this policy is located.

Student Information

Fathom® uses Student Information for the sole purpose of providing credentialed user access and operation of the Fathom digital platform. Fathom does not collect student information nor create or keep student profiles for non-educational purposes. Student Information shall mean personally identifiable information (PII) of a student and their "education records" as defined in the Family Educational Rights and Privacy Act ([FERPA](#)) 20 U.S.C. § 1232g and Personally Identifiable Information as defined in the Children's Online Privacy Protection Act of 1998 ([COPPA](#)) 15 U.S.C. § 6501-6506.

Fathom does not require first names, last names, or email addresses when creating student accounts – only username and password are needed for credentialed access. However, the normal student information needed by and shared with Fathom by teachers and school administrators usually include: first name, last name, email or username, password, and grade. The decision to include data beyond username and password is recommended but at the discretion of school administrators.

Fathom also collects indirect identifiers that are 'technical' and 'non-personal' which do not enable identification of an individual student. This type of information is collected as part of the standard operation of the platform. This may include IP address, browser type, device type & operating system from which the application was accessed. In addition, Fathom may collect information about browsing behavior, such as the date and time of access, the areas or pages visited, the amount of time spent viewing each page, the number of times returned to the application, the referring web page, pages visited, location, mobile carrier, device, and application IDs. Fathom analyzes de-identified, non-personal information and/or aggregated data solely for the purpose of improving service. No information at any point will be transferred or sold.

Student Privacy Pledge

Fathom is a proud signatory of the [Student Privacy Pledge](#), sponsored by The Future of Privacy Forum (FPF) and Software & Information Industry Association (SIIA). As a signatory, Fathom reaffirms its commitment to "safeguard student privacy regarding the collection, maintenance, and use of student personal information." It joins several other K-12 education technology companies that also share the same concerns and responsibilities.

The Student Privacy Pledge signees are held accountable to:

- Not sell student information
- Not behaviorally target advertising
- Use data for authorized education purposes only
- Not change privacy policies without notice or choice
- Enforce strict limits on data retention
- Support parental access to, and correction of errors in, their children's information
- Provide comprehensive security standards
- Be transparent about collection and use of data

COPPA Compliance

Fathom complies with the provisions of the Children's Online Privacy Protection Act ([COPPA](#)). COPPA imposes restrictions on how websites collect information from children 13 and under. The key goals of COPPA are to place parents in control over what information is collected from their children online and to protect children while recognizing the dynamic nature of the Internet. Information collected is used for the sole purpose of providing access to and usage of the Fathom system. Fathom will not require children to disclose more information than is reasonably necessary to participate in an activity as a condition of participation in the Fathom system. Parents can review their children's personal information, ask to have it deleted, and/or refuse to allow Fathom any further collection or use of their children's information by directing their request to: compliance@fathomreads.com.

FERPA Compliance

Fathom takes numerous measures to maintain the security and confidentiality of all student records and comply with requirements of the Family Educational Record Privacy Act ([FERPA](#)) applicable to the educational records of students. We will not use any information provided for the creation and maintenance of students' backpack accounts for any purpose other than preserving seamless access to licensed materials, and we will not disclose such information to any third party unless required by law. Any Student Information collected online or otherwise is used solely for the contracted purposes of the Fathom system. Fathom will not use nor sell Student Information for the purposes of marketing to students.

Storage of Student Information

Student Information is only stored and served from Fathom's dedicated cloud server hosted by Liquid Web data center, which has comprehensive monitoring systems in place using industry best practice tools ([Liquid Web Certifications](#)).

District & School Sharing of Student Information

Fathom offers two types of access: guest and credentialed.

1. Guest Access uses a single, school defined, shared password and does not require student information. It offers basic library access with no user accounts.

2. Credentialed Access (recommended) with individual user accounts is required for advanced book features, usage tracking, and access to user dashboards, Fathom's integrated Learning Management System (LMS), Assignment System, & Chat System.

User accounts may be created by the district, school, end-user, or Fathom. Frequently, the district requests Fathom's assistance with this step. The district has many options for communicating Student Information to Fathom. The information may be shared by automation via (1) third-party rostering services including: Canvas, ClassLink, Clever, Google Classrooms, Microsoft Education, and Schoology; or (2) by sending an Excel file of School Admins, Teachers, Students, Classes, and Class Enrollment Information to Fathom support for review and import. When transferring Student Information, Fathom uses appropriate TLS/HTTPS encryption.

Password Security

User passwords at rest on our dedicated cloud server are protected using salted hashes and are therefore not visible to those with server access. User authentication is protected by TLS/HTTPS encryption. When user passwords are provided by Schools on our excel roster import template, the files are deleted after importing to our server. As part of the import process, passwords are salted. The required strength of passwords has been set as a function of the assessed risk by user type. With our 6 third-party rostering services, no password information is shared with us.

Secure Infrastructure

Fathom has implemented administrative, physical, and technical infrastructure, as well as procedural safeguards, to protect and maintain the integrity of Student Information. Student information is only found on our dedicated cloud server and is not stored at our facility. Security software at our facility and on our servers is kept up-to-date with the latest definitions. Fathom is PCI-DSS compliant.

Employee and Third-Party Access

Access to Student Information is limited to: (1) District Administrators, School Administrators, and Teachers all having credentialed license access; (2) Fathom customer support staff on a need-to-know basis; and (3) a limited number of third-party, Website Developers who work exclusively on the Fathom platform. The identity of all employees and third-party contractors having access to Student Information is documented. The Fathom Cybersecurity Policy, the Fathom Privacy Policy, and the Student Privacy Pledge are part of Fathom's comprehensive training program. All employees and our third-party web developers with access to student information either through the website or behind the scenes working on our dedicated cloud server, must annually acknowledge in writing that they have been trained, are aware, and do commit to adhere to all Fathom policies regarding the safeguard of student information as well as pertinent state and federal regulations.

Student Information Security Breach Response

In the event of an unauthorized disclosure of Student Information, unauthorized access, or other incident that threatens the security of Student Information comes to Fathom's attention, the district and affected schools will be notified immediately. Fathom's Computer Security Incident Response Team (CSIRT) deals with security incidents as recommended by the Handbook for Computer Security Incident Response Teams (CSIRTs), published by the Software Engineering Institute, Carnegie Mellon University.

In the case of a security breach, Fathom's CSIRT is trained to:

- Make an initial assessment
- Communicate the incident
- Contain the damage and minimize the risk
- Identify the type and severity of the compromise
- Protect evidence
- Notify external agencies if appropriate
- Recover systems
- Compile and organize incident documentation
- Assess incident damage and cost
- Review the response
- Update policies

By submitting a written request to Fathom's point of contact, in regards to incident investigation, schools may request log data for end-user, administrative, and maintenance activity. Fathom carries cyber liability insurance to cover Crisis Management and Computer System Extortion, Media and Content Liability, and Security and Privacy Liability.

Disposal of Student Information

Student data is retained for two years after license expiration after which it is deleted. However, Fathom will always delete any Student Information, anytime upon district, school, or parent request.

Disclosure of Student Information

Fathom does not disclose student information collected from children or administrators for account creation to any third party unless required by law or court order.

Successor Entities

Should a successor entity acquire part or all of Fathom's organization in the future, they will be required to act in accordance with Fathom's Privacy Policy and consistent with Student Pledge principles or allow users a choice to send information to the future entity or have their information deleted.

Notice of Changes to Privacy Policy

This Privacy Policy was last reviewed and/or modified on May 17, 2023. All users will be notified when substantive changes are made. A banner will be displayed the first time users log on following the change. It will include a prominent statement stating that the policy has been changed and users are providing consent by continuing to use the service. A link to the revised policy will be included. Please contact us with questions or comments about this policy by email: compliance@fathomreads.com.