SECURITY OVERVIEW

SpecialNeedsWare, Inc. dba Ori Learning · Version v2026.09 · Effective September 23, 2026

This page summarizes the Security & Incident Exhibit to our Data Privacy Addendum. It is written for parents, students and school staff and is not a contract; the Exhibit controls, and districts receive it under the confidentiality terms of their agreement.

Our security program. Ori Learning maintains a written information security program for the student and staff data that schools entrust to us, as the Children's Online Privacy Protection Act rule (16 C.F.R. §312.8) requires of an operator. Our Chief Technology Officer, as our Security Officer, coordinates the program, holds the technical controls and leads incident response; our Privacy Officer is our designated privacy contact at legal@orilearning.com, which we read on business days; our Chief Executive Officer is accountable for the program and reviews incident notices where practicable. The program provides for an evaluation at least once a year and after any material incident or change. We use the NIST Cybersecurity Framework 2.0 as a reference for organizing and assessing it; the framework is a reference, not a certification.

Where data lives. The Ori Learning platform is hosted on Microsoft Azure in a single United States region; we do not operate our own data centers. The companies that process student or staff data for us, what each does, what it receives and where it processes are listed on our Subprocessor Schedule (orilearning.com/legal/subprocessors/), which is also Exhibit 2 to our Data Privacy Addendum; it lists the companies we have identified, and we add any further one we identify.

Who can access data. Every user signs in with a username and password or through the single sign-on a district chooses (Google, Microsoft, Clever or ClassLink). The platform is designed and configured to limit access by role and by the district's organization, schools and classes. Our own staff receive access to production data only for their duties, individually authenticated. We keep a list of the names and positions of the people at Ori Learning who may access student data and give it to a district on request.

Encryption. Every connection to the platform uses HTTPS, and Azure encrypts every production data store at rest, including the platform's database and file storage. We additionally encrypt names, usernames, email addresses, telephone numbers and external identifiers at the field level before they are written to the database, with keys held in Azure Key Vault.

Monitoring and recovery. A managed information-technology and security provider protects, monitors and patches our endpoints and infrastructure; it receives no flow of student data. Application and database activity logs record activity in the platform. Azure backs up the platform's database automatically on its schedule, keeps backups for a limited period on a rotating basis and states that it encrypts them; backups are used only to restore the platform as a whole. We maintain a business continuity and disaster recovery plan. The platform contains no generative artificial-intelligence feature.

Our people. Everyone at Ori Learning who has access to student or staff data has completed training on our security, incident and retention policies and on confidentiality under FERPA, COPPA and IDEA, and has signed a confidentiality agreement. Anyone new completes both before receiving access.

Our vendors. We evaluate each Subprocessor before it receives student or staff data, and our Subprocessors work under written terms that require them to protect it consistent with our commitments and limit their use to providing their services to us; we do not authorize any of them to use student data to train artificial-intelligence models. The services platform pages load, such as fonts, receive the network information a browser sends with any web request; we evaluate each and use them only in compliance with the law.

If something goes wrong. Our Incident Response Plan sets who does what. We notify a district without unreasonable delay, and no later than 72 hours after we confirm an unauthorized release of its student data, unless a law-enforcement agency directs a delay, in which case we notify the district as soon as the agency permits; a shorter period in the district's agreement or the law applies. We update the district as material facts become known and, on its request after the incident is resolved, give it a written summary of the cause and the remediation. Notices go to the privacy and security contact the district names and its designated fallback. We notify a district of an unauthorized acquisition of its other data when and as the law requires. We preserve evidence, cooperate with the district's investigation, and help it with any notices its own law requires. The district, not Ori Learning, decides how its parents and students are notified, unless a law places that duty on us. In this overview, "business days" means Business Days as the Ori Learning Definitions define them.

What we do not claim. We do not claim a certification, an audit report or a completed independent test that we do not hold; when we hold one, we state it in the Exhibit this page summarizes, and we answer any district's question about it directly.

Questions. Districts may ask any question at legal@orilearning.com, and may request our questionnaire responses as our Data Privacy Addendum provides. The full Security & Incident Exhibit, with the status of every control and the dates of the further commitments we have adopted, is provided to districts under the confidentiality terms of their agreement, and a district may post it as its own public-records law requires.