



Student Privacy and Security Overview

Our top priority in SOLARO's architecture since day one has been student privacy and security. Through prudent practices of SSL, tokenization, and abstraction; SOLARO has taken every possible precaution to protect the security of student data while also providing 24/7 access to students from web or mobile devices, anywhere in the world.

Privacy

Castle Rock Research provides a complete Privacy Policy for SOLARO that is publicly accessible at the following URL:

<http://www.castlerockresearch.com/privacy-policy>

The main takeaways from this policy are as follows:

- Castle Rock Research does not provide access to, license, or share any student data with any third-party company or government agency.
- Access to student data is restricted only to those employees or contractors of Castle Rock Research that require it to fulfill their function in the organization.
- Private information such as passwords is stored in such a way that they can never be accessed by any individual of Castle Rock Research. The only method of retrieving a student's password is to reset and provide them a new one (more about this in the Security section of this document).
- SOLARO is split into multiple databases that use tokens to pass data between them, meaning that student data is even further obscured from external sources (more about this in the Security section of this document).
- SOLARO does not display advertising to any of its users, so it does not expose any student information for ad targeting or demographic purposes.

For additional questions or concerns, please contact our Privacy Officer at privacy@solaro.com.



Security

Castle Rock Research has built SOLARO with industry-standard secure services and encryption. SOLARO also has several key architectural features that ensure secure retention and access to student data.

Limited Information Capture

SOLARO does not require significant amounts of personal student information to deliver its value. Therefore, SOLARO prevents users from entering more info than is strictly necessary to function.

COPPA Compliance

SOLARO's student accounts are created in a process that fully complies with COPPA. Implied parental consent is given if a Teacher or School Administrator creates an account for a student, and if a parent wants to create an individual account for their child, a credit card purchase is required. Anonymous usernames and accounts are provided to students for non-educational institutions such as libraries.

Tokenization

SOLARO segregates all personal identifying information for a student from their data:

1. Students provide their usernames and passwords to log in, but that information is sent to a separate server with a separate database for authentication.
2. Once authenticated, a token is provided back, which is used to access the main SOLARO server and database. This token is completely anonymous and expires after a period of inactivity.
3. Once a token has expired, all access to the SOLARO server and database is restricted until the user re-authenticates.

This segregation means that, even if a third-party were to gain full access to the SOLARO database, they could not pinpoint a specific account or token with its corresponding data.

Any further questions or concerns about the security of SOLARO can be directed to Mathieu Lavoie, Vice President of Technology, at mlavoie@castlerockresearch.com