SchooLinks Data Security and Privacy Plan

This document outlines SchooLinks Data Security and Privacy Plan. Protocols and procedures might change based on industry best practices.

Data Security

SchooLinks follows guidelines and best practices set forth by the Open Web Application Security Project (OWASP) to ensure that our application and infrastructure are secure.

Security measures include, but are not limited to VPN-only access of data and infrastructure, restriction of access by IP address, password protection with stringent complexity requirements, regular password rotation, regular access key rotation, and two-factor authentication. SchooLinks' data is encrypted at rest and in transmission and all user-data is transmitted via TLS 2.0 or later secured connections. We maintain rate-limiting and lock-out mechanisms to protect against brute force attacks. Additionally, we perform daily backups that are stored separately from the database infrastructure to ensure data access in the event of a ransomware attack.

At the application level, SchooLinks has role-based permissions that can restrict access or view of district users to student data on a need to know basis. Access can be restricted at a module level, field level, or based on scope of student access. By default users are granted access according to the Principle of Least Privilege.

SchooLinks infrastructure is entirely cloud-based. We use Amazon Web Services (AWS), which has industry-leading security practices. Where possible, SchooLinks leverages AWS's managed services instead of stand-alone cloud server instances. This dramatically lowers the risk-profile and decreases the potential attack surfaces.

SchooLinks undergoes regular security audits and penetration tests by third-party providers to ensure the security of the application and service offerings. SchooLinks keeps all software packages and dependencies up to date with the latest versions to ensure access to all security patches.

When interchanging student data with districts and partners, SchooLinks does not allow sending of data through email and instead interchange data through secure APIs or an SFTP server that SchooLinks maintains for secure data interchange with its partners. SchooLinks trains its employees and communicates with its district partners about best practices to prevent any social engineering or phishing attacks.

In our application layer, all user-supplied inputs via the UI and in data files passed via SFTP are sanitized to prevent SQL injections or XSRF attacks by default within the framework that we use.

How we ensure information privacy

SchooLinks never sells or provides any student or district data to third parties.

SchooLinks restricts internal access to and usage of data. SchooLinks does not use it for internal development or testing purposes. Only select individuals within the company who deal directly with the support of a particular account can view and access its data. SchooLinks has both application-level restrictions and safeguards and internal policies to prevent unauthorized internal access to this data for purposes other than support and troubleshooting. Access to and changes to this data within our internal administration portal is logged based on user and IP address.

When SchooLinks needs to conduct analytics studies of usage of the platform, SchooLinks only uses anonymized, non-personally identifiable data.

Following the termination of a contract, SchooLinks destroys all school district data from its system, in accordance with all state and federal regulations and/or district's data sharing agreement.

More detailed information about how we detail with particular district's data may be specified in Data Sharing Agreements signed with SEAs or LEAs.

Link to public Privacy Policy on homepage: https://www.schoolinks.com/privacy-policy

Last Updated January 10th, 2023