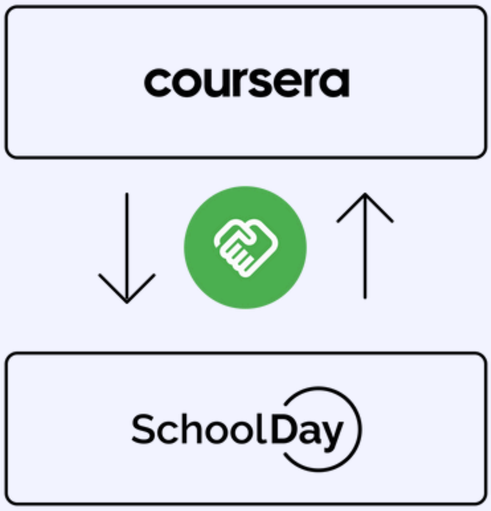
SCHOOLDAY CUSTOMER STORY

Enabling Career Pathways Without Compromising Student Privacy

A case study of a large U.S. School District, Coursera and SchoolDay



OVERVIEW

One of the top-10 school districts in the U.S. partnered with Coursera and SchoolDay to deliver a secure, scalable, and privacy-compliant capstone learning experience for high school students. By leveraging SchoolDay's self-sovereign ecosystem orchestration platform, this district successfully offered Coursera Career Academy courses while safeguarding student privacy and maintaining a seamless user experience for students, educators and administrators.

This partnership demonstrated that districts can expand access to high-quality third-party learning opportunities without exposing students' personally identifiable information.

CHALLENGE: ENABLE LEARNING WITHOUT EXPOSING STUDENT PII

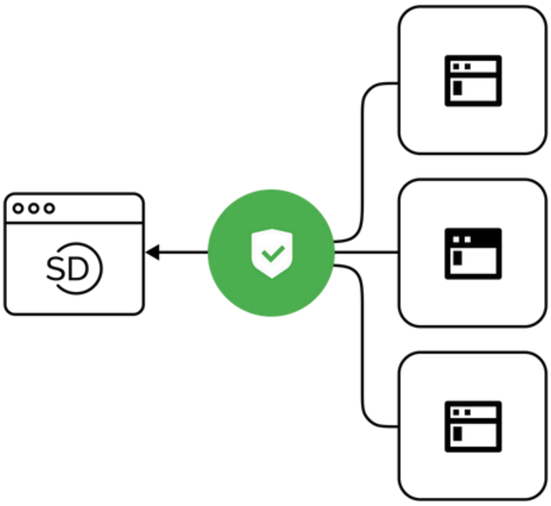
As the school district sought to integrate Coursera's career-focused curriculum into its high school capstone program, it faced a critical challenge: how to protect its students' Personally Identifiable Information (PII) while enabling third-party access to learning tools and generating usable performance reports.

SOLUTION: TOKENIZATION OF STUDENT DATA THROUGH SCHOOLDAY

SchoolDay implemented a deep linking integration between Coursera and the school district's LMS, Schoology. Through this connection, student PII was tokenized at the point of enrollment, replacing sensitive identifiers (e.g., name, email) with unique, anonymized tokens.

- ✓ Students enrolled in Coursera courses via the Schoology LMS.
- ✓ SchoolDay replaced student PII with secure tokens at enrollment.
- ✓ Coursera operated entirely on anonymized student data.

When authorized educators viewed progress reports, tokens were detokenized locally using the SchoolDay platform, reassociating them with the correct student only on the viewing device.



What Is PII Tokenization?

Personally Identifiable Information can be protected by avoiding direct data sharing with third parties. Instead of passing real credentials to target applications, a format-preserving token is passed, which authorizes the incoming user to access the application. In the case of PII, the sensitive data is replaced with a token or string of meaningless but unique characters. For example, a student's name, such as John Smith, might be replaced in the receiving application's data store with a **format-preserving token**, such as "D-ggf'xzdnmla".

To make tokenized data usable for stakeholders, it must eventually be detokenized. Since most modern applications are browser-based and deliver information through webpages, SchoolDay provides a way to display detokenized data directly in the user's browser—without the application provider's involvement and without the data ever passing through their network or servers.

The PII data is sent to the end-user as **tokens.** The SchoolDay platform intercepts the incoming tokens and replaces each with the actual PII on the local device. In this manner, the token is deanonymized only when received on the local device.

IMPLEMENTATION

Course Selection: A managing teacher selected relevant Coursera Career Academy courses tailored to the district's capstone requirements.

Privacy Setup: SchoolDay enabled token-based enrollment via deep linking, shielding student data across the Coursera ecosystem.

Monitoring & Reporting: Teachers tracked student progress using Coursera's reporting tools. Tokenized data was deanonymized only when viewed locally by authorized staff.

Certification: Upon course completion, certificates were issued to anonymized accounts. Students could later request name updates via a verification process.

RESULTS

- Students successfully participated in the program, enrolling in numerous Coursera courses.
- All participants earned certificates for the courses they completed.
- No personally identifiable information was exposed to Coursera or any third-party systems.

The process demonstrated that tokenized identities can enable scalable partnerships between districts and edtech vendors without compromising student privacy.

BENEFITS

Student Privacy: Student PII was never shared with third parties.

Ease of Integration: Students and teachers accessed courses seamlessly through LMS deep linking.

Meaningful Reporting: Stakeholders received personalized and actionable insights without exposing sensitive data.

Scalability: The framework supports future expansion across other partners and districts.

CONCLUSION

This case study demonstrates how SchoolDay's tokenization approach enables districts to securely partner with edtech vendors while maintaining full control over student data. By using tokenized identities and local detokenization, districts can expand digital learning opportunities without compromising privacy, compliance, or trust.

schoolday.com
info@schoolday.com
888.557.6085

SchoolDay