

Policies and Practices

Student Data Privacy & Security Primer

West's Education group, part of West Corporation and the provider of SchoolMessenger solutions, is committed to safeguarding the privacy and security of customer information. We believe the personal information of our school customers and users is private, treat this information confidentially, and are committed to its security.

To support our school customers and their stakeholders, we provide this primer to outline our privacy policies, our related resources, and several third-party resources. In combination, we hope this information will provide educators, parents and community members with a starting point to understand how SchoolMessenger solutions safeguard student personal information as well as where to turn for further guidance and best practices.

West's Education Group Privacy Policies

In general, for our SchoolMessenger solutions:

- We will not ask for or collect personal information unless necessary to deliver our service or respond to a request;
- We will not use or share personal information with anyone except to deliver our services, comply with the law, protect our rights or the safety of our users, or as otherwise directed by our customers and users;
- We do not sell, trade, lease or loan student personal information to any third party for any reason, including for marketing or advertising; and
- We use industry standard measures to help protect personal information against unauthorized access and use.

Additional detail regarding our use of student personal information and other user information is described in our Privacy Statement (<http://www.schoolmessenger.com/privacy-statement>).

West's SchoolMessenger solutions are a signatory to the Student Privacy Pledge (www.studentprivacypledge.org), which legally binds us to a dozen commitments regarding the collection, maintenance, and use of student personal information.

SchoolMessenger Communicate has been awarded the iKeepSafe Privacy FERPA Badge, providing schools with an independent, trusted review of alignment with iKeepSafe's FERPA evaluation program guidelines (<http://ikeepSAFE.org/participating-companies>).

School Best Practices

Schools have rounded the turn in the journey toward digital learning, but often a large gap remains around privacy and security. Maintaining confidentiality requires a comprehensive set of policies and practices. West's Education group recently released a free best practices guide to help educators address school and student data privacy. "School and Student Data Privacy: Nine Considerations for Community Engagement" provides a comprehensive overview of school and student data privacy best practices, policies and procedures.

It outlines nine best practices for school and student data privacy:

1. Legal Compliance is the Floor to Building School Norms and Culture
2. Conduct an Internal Assessment to Benchmark Current Practices Against Regulations and Norms
3. Governance & Accountability Provide a Framework for the Safeguarding of Student Data
4. Transparency & Communication Should Extend to Parents

5. Support Parents in their Data Access & Awareness of Related Rights
6. Student Privacy Requires Data Security
7. Schools Should Direct Third-Party Vendor & Partner Data Access
8. Staff Awareness & Training Is Essential
9. Student Education Reinforces Good Practice

This paper is available for free at <http://www.schoolmessenger.com/student-data-privacy-best-practices/>

In addition, West's Education group hosted a related webinar featuring West and third-party experts. The webinar is archived and available for free at <http://www.schoolmessenger.com/resources/>

Additional Resources

Consortium for School Networking (CoSN):

- CoSN Trusted Learning Environment Seal Program TrustedLearning.org
- CoSN Protecting Privacy in Connected Learning Toolkit <http://www.cosn.org/focus-areas/leadership-vision/protecting-privacy>
- CoSN Protecting Privacy in Connected Learning Online Course <http://www.cosn.org/privacy-course-syllabus>

Data Quality Campaign: <http://dataqualitycampaign.org/> & <http://dataqualitycampaign.org/topic/safeguarding-data/>

Future of Privacy Forum: <https://fpf.org/issues/k-12-education> & <https://ferpasherpa.org>

iKeepSafe: <http://ikeepsafe.org/privacy/>

National Association of Secondary School Principals: <https://www.principals.org/who-we-are/board-of-directors/position-statements/student-data-privacy>

PlayWell Privacy Trust Framework: <http://playwell-llc.com/privacy-framework/>

Software & Information Industry Association: <http://www.siiia.net/Divisions/ETIN-Education-Technology-Industry-Network/Resources/Student-Privacy-Data-Security-Toolkit-for-School-Service-Providers>

Strive Together: http://www.strivetogether.org/sites/default/files/StriveTogether_Student_Data_Privacy_Best_Practices.pdf

Student Privacy Pledge: <https://studentprivacypledge.org/>

U.S. Department of Education, Privacy Technical Assistance Center: <http://ptac.ed.gov>

10 Foundational Principles for Using and Safeguarding Students' Personal Information: <http://studentdatapinciples.org/the-principles/>