

AI Safety & Privacy Standard for Schools

WHAT IS THE AI SAFETY & PRIVACY STANDARD

The American Federation of Teachers (AFT) and Microsoft Corp. have agreed upon a landmark AI Safety & Privacy Standard that establishes protections AI use in education. The Standard is designed to protect students, educators and families and allows any school in America to incorporate these protections into their agreements with Microsoft and hold Microsoft accountable to them.

WHY THE STANDARD IS NEEDED

Students, families, and educators deserve technology that protects privacy, strengthens safety, and keeps people in control. These commitments reflect principles Microsoft has long championed. We believe the AFT Safety & Privacy Standard creates clear guidelines for how AI should be used in schools. This gives parents and educators greater confidence while requiring AI companies to meet higher standards for safe, responsible and privacy-protecting AI in schools.

At its core, the agreement turns shared principles into clear, enforceable protections centered on three priorities:

Protecting Privacy

Educators, parents and students can have confidence that data remains protected. Student and educator data will not be used to train AI models, will never be sold or used for advertising, and schools maintain control over how data is used, retained, and deleted.

Enhancing Safety

Students and educators are protected by strong security, safeguards, and human oversight. AI systems must be designed to avoid harmful or manipulative experiences, protect sensitive information, and meet rigorous standards for security, accountability, and responsible use.

Providing Transparency and Control

Families can expect clear, accessible information about how AI is being used in schools and their safeguards, including what data is collected, and what protections are in place. Schools control when and how AI is used, and providers need to communicate clearly about product changes, risks, and controls.

MICROSOFT'S COMMITMENT

For Schools

Beginning November 1, 2026, Microsoft will make the protections offered in the AI Safety & Privacy Standard available to every school district in the United States. Districts can add them to new or existing agreements with Microsoft, with no contract renegotiation or renewal required. The protections are contractually enforceable if those commitments are not met.

For Educators & Families

Microsoft will provide education leaders and families with clear, plain-language information about how our AI products work in the classroom, the controls schools have over them, and the safeguards that protect students. Parents deserve straightforward information about the technology used in their schools.

AI Safety & Privacy Standard at-a-glance

There are 10 contractually enforceable protections for schools included in the AI Safety & Privacy Standard:

01 No training on student or educator data

Student, educator, and customer data cannot be used to train or improve an AI model, apart from a narrow safety and security exception.

02 Data minimization by design

Products collect only what they need. Tracking, profiling, biometrics, memory, and higher-risk features require limits and review.

03 Customer data ownership

Customers and students own their data. It cannot be sold or used for ads or product development; customers control export, retention, and deletion.

04 Human oversight and explainability

AI supports, people decide. High-risk decisions require human review. AI companions are prohibited.

05 Real accountability

Providers maintain certifications, report breaches within 72 hours, and fix violations, or AI use is paused or ended.

06 Security that matches the stakes

Data is encrypted, access-controlled, independently tested, and covered by incident-response plans, including for subprocessors.

07 Meaningful consent and transparency for families

Families receive clear, plain-language guides explaining how the AI products work and address privacy, safety, and security.

08 Equity, accessibility, and inclusion

Products must be accessible and fair. Providers disclose and fix gaps, offer equal features, and fund an independent study.

09 No feature creep and no vendor lock-in

Customers control material new features and data use, receive notice, and can export data and switch providers freely.

10 Long-term data responsibility

Data is kept only as needed. Training and sale bans are permanent. Deletion and breach duties continue after the contract ends.

This document is provided for informational purposes only and is intended as a summary for educators, administrators, and families. Please refer to the [AFT AI Safety & Privacy Standard](#) for the complete terms, commitments, and requirements.