



Student Information Systems (SIS) & Learning Management Systems (LMS)

Best Practices, Common Issues, and Practical Solutions for K-12 Schools

Introduction

Student Information Systems (SIS) and Learning Management Systems (LMS) form the digital backbone of today's schools. These platforms store sensitive student data, manage classroom activities, and support daily communication between teachers, parents, and administrators.

When well managed, they improve efficiency and learning outcomes. When poorly configured, they can create frustration, data risks, and downtime.

This guide outlines key best practices, common issues, and actionable steps schools can take to ensure these systems remain reliable, secure, and aligned with educational goals.

Best Practices for Managing SIS and LMS Platforms

1. Prioritize Data Security & Privacy

- Ensure systems comply with **FERPA** and **state privacy laws**.
- Require **Multi-Factor Authentication (MFA)** for admin and teacher accounts.
- Limit access by role — teachers, students, and administrators should have distinct permissions.
- Encrypt data both in transit and at rest.

2. Keep Systems Updated

- Schedule regular **software updates and patches** to address vulnerabilities.
- Document all system versions and plugin compatibility.
- Test updates in a sandbox environment before applying them district-wide.

3. Integrate Systems Strategically

- Sync SIS and LMS platforms to avoid manual data entry (e.g., PowerSchool ↔ Canvas, FACTS ↔ Google Classroom).
- Use **Single Sign-On (SSO)** to reduce password fatigue and security risks.
- Work with vendors to ensure API connections are secure and supported.

4. Train Staff and End Users

- Provide annual training for teachers and administrators.

- Develop quick reference guides for common tasks (grade submission, attendance, reports).
- Encourage teachers to explore analytics and reporting features to improve instruction.

5. Establish a Support & Maintenance Plan

- Assign a point of contact for system issues or escalations.
- Monitor uptime, latency, and user feedback.
- Maintain vendor support contracts and escalation channels for critical incidents.

Common Issues Schools Face

Issue	Root Cause	Solution
Duplicate or missing student records	Inconsistent data entry or sync errors	Automate imports from SIS to LMS and enforce uniform naming conventions.
Slow system performance	Outdated hardware or overused shared servers	Upgrade hosting environment or enable content caching.
User login issues	Poor password management or SSO misconfiguration	Enable password reset self-service and verify SSO settings.
Data breaches or exposure	Weak access controls or improper sharing	Implement MFA, audit permissions quarterly, and restrict export functions.
Low adoption by teachers	Lack of training or system complexity	Offer ongoing PD sessions and highlight time-saving features.
Integration failures	API or plugin version conflicts	Test updates before rollout and maintain version documentation.

Actionable Solutions

- Conduct a **biannual system audit** to verify user permissions, data integrity, and performance.

- Use a **staging environment** for testing new features or integrations before deploying live.
- Implement a **backup and recovery policy** specifically for SIS/LMS databases.
- Review **vendor SLAs (Service Level Agreements)** to ensure they meet uptime and security standards.
- Maintain an **incident log** to track and resolve recurring issues.

Cybersecurity Considerations

Because SIS and LMS platforms hold sensitive personal data, they should be included in your school's **cybersecurity plan**.

- Require secure HTTPS connections and trusted certificates.
- Regularly review audit logs for unauthorized data exports.
- Set alerts for multiple failed login attempts or unusual activity.
- Coordinate with your IT provider to include SIS/LMS in network monitoring.

Conclusion

Your SIS and LMS systems are vital to both education and operations. With regular maintenance, strong data practices, and trained staff, these platforms can streamline processes, enhance learning, and maintain the highest standards of data protection.

