CyberSphere SOLUTIONS

AI Safety & Data Privacy in Schools

Using Artificial Intelligence Responsibly in Education

Introduction

Artificial Intelligence (AI) tools are transforming how schools manage operations, teach, and engage students. From automating administrative tasks to supporting personalized learning, AI offers enormous potential.
However, it also introduces new risks around **data privacy, student safety, and ethical use**. This guide outlines key points every educator and IT leader should know to ensure AI tools are used securely and responsibly.

1. How AI Models Use Data

Most AI platforms learn by analyzing vast amounts of information, often text, images, or data entered by users.
When you use an AI tool:

- The information you enter may be **stored temporarily or permanently** to improve the model.
- Some tools use your input to **train future versions** of the system.
- Unless specifically stated, the platform may **not be FERPA-compliant**.

Important: Never assume that an AI tool automatically protects personal data. Always review the provider's **privacy policy** and **data retention settings** before use.

2. What's Safe to Share and What's Not

AI can assist with lesson plans, reports, and communications, but caution is essential.

Safe to Share:

- General prompts (e.g., "Create a science quiz for middle school students").
- Non-identifiable classroom content or curriculum ideas.
- Publicly available information that doesn't contain private records.

Never Share:

- Student names, grades, or personal identifiers.
- Attendance, health, or disciplinary records.
- Login credentials, school database access details, or internal documents.
- Photos or videos of students without explicit consent.

When in doubt, **treat AI tools like a public forum.** If you wouldn't post it online, don't enter it into an AI system.

3. Student Data & FERPA Compliance

Under the **Family Educational Rights and Privacy Act (FERPA)**, schools must protect personally identifiable information (PII) and only disclose it to authorized parties.
To stay compliant when using AI:

- Use **district-approved tools** that meet FERPA and state privacy standards.
- Require vendors to sign **data privacy agreements** before implementation.
- Store all generated content (lesson plans, analytics, etc.) within school-controlled systems.
- Educate teachers about how AI may collect and store student information.

Remember: **AI convenience should never outweigh student privacy.**

4. Best Practices for Educators Using AI Tools

1. **Check approval status** – Verify whether the AI tool is approved by the IT department.
2. **Use school accounts** – Avoid signing up with personal emails.
3. **Avoid sensitive data** – Never include identifying student or staff details in prompts.
4. **Review outputs carefully** – AI responses may contain errors or bias; always verify accuracy.
5. **Update privacy settings** – Disable data-sharing or training features when possible.
6. **Train staff and students** – Provide basic digital literacy and privacy awareness training.
7. **Document use cases** – Keep records of AI systems used for transparency and accountability.

Closing Note

AI is a powerful ally in education when used with care. By applying thoughtful guidelines and prioritizing privacy, schools can embrace innovation without compromising trust or compliance.