FERPA Compliance Checklist

Protecting student privacy in behavior data collection

classroompulse.io

FERPA Basics for Behavior Data

FERPA (Family Educational Rights and Privacy Act) protects the privacy of student education records, including behavior data collected as part of the educational process.

Data Collection Compliance

- [ ] Behavior data is collected for legitimate educational purposes
- [ ] Only staff with educational need have access to data
- [ ] Data collection methods are documented
- [ ] Parents have been informed of data collection practices
- [ ] Student identifiers are protected

Storage Requirements

- [ ] Digital records are password-protected
- [ ] Physical records are in locked storage
- [ ] Data is stored on school-approved systems only
- [ ] Cloud storage meets district security requirements
- [ ] Backup procedures are in place
- [ ] Retention schedules are followed

Sharing Restrictions

- [ ] Written consent obtained before sharing with outside agencies
- [ ] Directory information policies followed
- [ ] Need-to-know basis for internal sharing
- [ ] Transfer procedures followed when student changes schools
- [ ] Redaction procedures used when required

Parent Rights

- Right to inspect and review all education records
- Right to request amendment of inaccurate records
- Right to consent before disclosure to third parties
- Right to file complaint with Department of Education

Important

Behavior data shared during team meetings should be limited to those with legitimate educational interest. Avoid discussing in public spaces.

Documentation Checklist

- [ ] Consent forms on file (if required)
- [ ] Access log maintained for sensitive records
- [ ] Staff training documentation current
- [ ] Data breach response plan in place

Compliance Notes

Secure Behavior Tracking

Classroom Pulse is built with FERPA compliance in mind. Role-based access, audit logs, and secure cloud storage included.

classroompulse.io/signup