



Florida Council of Independent Schools Data Protection & Data Sharing Agreement

Member School Data Submission and Use Policy

Last Updated June 5, 2026

Purpose

The Florida Council of Independent Schools (FCIS) collects institutional data from member schools in order to fulfill its mission of supporting, accrediting, and advancing independent schools in Florida. This agreement outlines how FCIS collects, uses, protects, and safeguards member school data.

1. Scope of Data Covered

This agreement applies to all data submitted by member schools to FCIS, including, but not limited to:

- FCIS Annual Census
- FCIS Accreditation Portal
- FCIS Inservice Portal
- FCIS Events Portal
- NAIS DASL-related data submissions
- Webinar registration and recording data
- Job Board submissions
- Any additional FCIS-operated systems or surveys

2. Data Stewardship

FCIS serves as a data steward and custodian of submitted information solely for purposes aligned with its mission and services.

3. Permitted Use of Data

FCIS uses submitted data exclusively for:

- Accreditation review and support
- Association reporting and aggregate trend analysis
- Member benchmarking (de-identified or aggregated)
- Operational support and program improvement
- Communication related to FCIS services and events
- Research supporting independent school leadership

Data may be reported in aggregated or anonymized formats for association-wide insights. Individual school data will never be publicly disclosed without explicit written permission.

4. Non-Disclosure to Third Parties

FCIS does **not**:

- Sell member data
- Share identifiable school data with third parties
- Provide member data to vendors for marketing purposes
- Use submitted data to train, improve, or contribute to Large Language Model (LLM) platforms
- Upload identifiable member data into public AI tools

5. Data Security Measures

FCIS implements reasonable and appropriate administrative, technical, and physical safeguards, including:

- Secure, access-restricted portals
- Role-based access controls
- Encrypted data transmission (HTTPS/SSL)
- Secure cloud hosting environments
- Routine system updates and security monitoring
- Limited internal staff access based on job function

Access to identifiable school data is limited to authorized FCIS personnel whose responsibilities require such access.

6. Data Retention

FCIS retains submitted data for an infinite timeframe to fulfill accreditation, reporting, historical analysis, and legal obligations. Archived data is stored securely.

7. Webinar & Recording Data

Webinar registrations and recordings are used for:

- Attendance tracking
- Professional development records
- Member access to session archives

Recordings may be shared with registered participants or member schools but will not be distributed externally without consent.

8. DASL Data

Any NAIS DASL-related data shared with FCIS is treated with the same level of confidentiality and security described above. FCIS does not redistribute school-level DASL data without authorization.

9. Compliance

FCIS is committed to complying with applicable federal and state data privacy regulations and best practices appropriate to its role as a membership association.

10. Questions & Contact

Questions regarding this agreement or data security practices may be directed to:

Evelyn McCulloch

Director of Technology and Accreditation Support

Florida Council of Independent Schools

emcculloch@fcis.org

Statement of Assurance

By submitting institutional data to FCIS systems, member schools acknowledge and understand that FCIS will handle such data in accordance with the protections outlined in this agreement.