KENTUCKY STATE UNIVERSITY

Policies and Regulations

POLICY TITLE:

Kentucky State University Online Student Privacy Policy

APPLIES TO:

- Kentucky State University Online Students Enrolled in Online Courses
- Faculty and staff who access, collect, or manage student information
- Third-party vendors and service providers with access to student data
- Student records maintained in any format

ADMINISTRATIVE AUTHORITY:

- Office of the Provost/Vice President for Academic Affairs
- Office of Online Education
- Registrar's Office

APPROVED BY:

- The President
- Academic Affairs
- The Office of Online Education
- The Kentucky State University Board of Regents

EFFECTIVE DATE:

6/12/2026

NEXT REVIEW DATE:

5/1/2028

POLICY STATEMENT:

Kentucky State University Online is committed to protecting the privacy, confidentiality, and security of student education records and personal information in accordance with the Family Educational Rights and Privacy Act (FERPA), applicable state and federal laws, and accreditation. This policy applies to all students enrolled in online, hybrid, and distance education programs, as well as traditional students using digital learning platforms.

This policy serves to:

- Ensure compliance with FERPA and other applicable privacy regulations

- Protect student education records and personally identifiable information (PII)
- Establish procedures for secure handling of student data in online environments
- Define responsibilities of faculty, staff, students, and third-party vendors
- Provide transparency regarding data collection and usage practices
- Maintain accreditation standards

DEFINITIONS:

Education Records: Records directly related to a student maintained by the institution or a party acting on behalf of the institution, including academic transcripts, enrollment records, financial aid information, disciplinary records, and records of online course activity.

Personally Identifiable Information (PII): Information that can be used to identify an individual student, including but not limited to: name, student ID number, Social Security number, date of birth, email address, telephone number, IP address, biometric identifiers, and photographs.

Directory Information: Information contained in student education records that generally would not be considered harmful or an invasion of privacy if disclosed, including student name, email address, major field of study, dates of attendance, enrollment status, degrees and awards received, and participation in officially recognized activities.

Legitimate Educational Interest: A demonstrated need to access student information to fulfill one's professional responsibilities related to instruction, advising, administration, or student support services.

Third-Party Service Provider: External vendors, contractors, or organizations that provide educational technology tools, learning management systems, or services that require access to student information.

Authentication: The process of verifying the identity of a student participating in an online course or accessing digital educational resources.

Student Rights under FERPA:

- Students enrolled at Kentucky State University Online have the following rights regarding their education records:
- **Right to Inspect and Review**: Students have the right to inspect and review their education records within 45 days of submitting a written request to the Office of the Registrar. This includes records maintained in the learning management system and other online platforms.
- **Right to Request Amendment**: Students have the right to request amendment of education records they believe are inaccurate, misleading, or in violation of their privacy rights. Requests must be submitted in writing with supporting documentation.
- **Right to Consent to Disclosure**: Students have the right to consent to disclosure of personally identifiable information from their education records, except in cases where FERPA authorizes disclosure without consent
- **Right to File a Complaint**: Students have the right to file a complaint with the U.S. Department of Education concerning alleged failures by the institution to comply with FERPA requirements:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-5920

- **Right to Opt Out of Directory Information**: Students may request that directory information not be disclosed by completing the Directory Information Opt-Out Form available through the Office of the Registrar. This request remains in effect until revoked by the student in writing.

Students who are 18 or older or are attending a postsecondary institution have full rights under FERPA. Parents or guardians do not have inherent rights to access student education records without the student's written consent.

The University may disclose education records to parents without student consent in the following circumstances:

- The student is claimed as a dependent for federal tax purposes (verification required)
- A health or safety emergency involves the student
- The student has violated laws or University policies concerning alcohol or substance abuse (if under age 21)
- The student has provided written consent for parental access

Data Collection and Use:

The University collects the following categories of student information through online learning platforms:

Category	Examples
Enrollment Data	Course registrations, enrollment status, program of study, academic level
Academic Performance	Grades, assignment submissions, quiz/exam scores, participation records, discussion board posts
Learning Analytics	Login frequency, time spent on course materials, page views, video watch time, quiz attempts
Communication Records	Email correspondence, messages within LMS, video conference recordings, chat logs
Authentication Data	User credentials, login times, IP addresses, device information
Financial Information	Tuition payments, financial aid status, account balances

Table 1: Categories of student data collected in online learning environments

Student information is collected only for legitimate educational purposes, including:

- Facilitating instruction and course delivery
- Assessing student learning and academic progress
- Providing academic advising and student support services
- Verifying student identity and preventing academic dishonesty

- Improving instructional design and course effectiveness
- Fulfilling institutional reporting and accreditation requirements
- Conducting educational research (with appropriate approvals)
- Ensuring compliance with federal and state regulations

The University adheres to data minimization principles by collecting only the information necessary and relevant for specific educational purposes. Unnecessary data is not collected, and information is retained only as long as required by institutional policy or legal mandate.

Disclosure of Student Information:

FERPA permits disclosure of education records without student consent in the following circumstances:

1. **School Officials with Legitimate Educational Interest**: Faculty and staff who need access to perform their institutional responsibilities
2. **Other Schools**: To institutions where the student seeks to enroll or is enrolled
3. **Authorized Representatives**: For audit or evaluation purposes related to federal or state educational programs
4. **Financial Aid Determinations**: In connection with student applications for financial assistance
5. **Accrediting Organizations**: To carry out accreditation functions
6. **Compliance with Judicial Orders**: In response to lawfully issued subpoenas or court orders
7. **Health and Safety Emergencies**: To protect the health or safety of students or others
8. **State and Local Authorities**: Within the juvenile justice system, pursuant to specific state law

All other disclosures of personally identifiable information require written consent from the student, specifying:

- The records to be disclosed
- The purpose of the disclosure
- The party or class of parties to whom disclosure may be made
- The student's signature and date

The University's Registrar Office maintains records of all disclosures of personally identifiable information (except disclosures to school officials and directory information), including the date, parties to whom disclosed, and legitimate interest for disclosure.

Data Breach Response:

A data breach is any unauthorized access, acquisition, use, or disclosure of student education records or personally identifiable information that compromises the security, confidentiality, or integrity of those records or information.

In the event of a suspected or confirmed data breach:

1. **Immediate Containment**: Affected systems are isolated to prevent further compromise
2. **Investigation**: IT Security conducts forensic analysis to determine scope and cause
3. **Notification to Leadership**: Privacy Officer and senior administration are immediately informed

4. **Legal Review**: General Counsel assesses legal obligations and liability
5. **Student Notification**: Affected students are notified within 48 hours when possible, including:
    - Description of the breach and information compromised
    - Steps the University is taking to address the incident
    - Protective measures students can take
    - Contact information for questions and support
6. **Regulatory Reporting**: Breach reported to appropriate agencies as required by law
7. **Remediation**: Security vulnerabilities are addressed and systems are hardened
8. **Documentation**: Comprehensive incident report prepared for review
9. **Post-Incident Review**: Lessons learned and policy updates implemented

Third-party service providers must notify the University within 24 hours of discovering any breach involving student data. The vendor's incident response obligations are specified in service agreements.

Complaints

Students, faculty, or staff who believe a privacy violation has occurred should report concerns to the Office of the Registrar.

All complaints are investigated promptly and confidentially:

1. Complaint is received and documented
2. Preliminary review determines if a policy violation occurred
3. Investigation conducted with interviews and evidence gathering
4. Findings documented and reported to the complainant and the relevant parties
5. Corrective action taken if the violation confirmed
6. Follow-up ensures resolution and prevents recurrence

Violations of this policy may result in disciplinary action:

- **Students**: Academic integrity violations, suspension, or expulsion under the Student Code of Conduct
- **Faculty and Staff**: Counseling, training, suspension, or termination under employment policies
- **Vendors**: Contract termination and legal remedies

REFERENCES AND RELATED MATERIALS:

CONTACTS:

Office of Online Education

HISTORY: