

BOARD OF REGENTS
for
KENTUCKY STATE UNIVERSITY



Meeting of the Board of Regents
Tuesday, March 3, 2026
1 p.m. ET

Julian M. Carroll Academic Services Building, 2nd Floor
400 East Main Street
Frankfort, Kentucky 40601

KENTUCKY STATE UNIVERSITY

MISSION STATEMENT

Provide transformative educational experiences to prepare graduates for making meaningful contributions to society.

Kentucky State University is a public, research-comprehensive, historically black, 1890 land grant institution.

KENTUCKY STATE UNIVERSITY

VISION STATEMENT

Foster Innovation and Inspire Leaders to Advance the Commonwealth and the World.

KENTUCKY STATE UNIVERSITY

CORE VALUES

- Compassion, Communication, Commitment, and Collaboration
- Ethical and Moral Responsibility
- Intentional Actions
- Excellence and Innovation
- Impactful Community Engagement
- Holistic Professional Development

KENTUCKY STATE UNIVERSITY BOARD MEMBERS

Ms. Tammi Dukes (2027)
Mr. Matthew Grimshaw (2030)
Mr. Edward Fields (2026), Staff Regent
Mr. Edward Hatchett, Esq. (2031)
Mr. Jason Moseley (2026)
Dr. Charles Moyer (2027)
Mr. Jonathan Rabinowitz, Esq. (2030)
Mr. Robert Ramsey, Sr. (2028)
Ms. Joan "Toni" Stringer, Esq. (2028)
Dr. James Obielodan (2028)

KENTUCKY STATE UNIVERSITY ELECTED BOARD OFFICERS

Ms. Tammi Dukes, *Chairperson*
Mr. Edward Hatchett, Esq., *Vice Chairperson*

Ms. Nicole Sergent, Esq., *Secretary*
Dr. Heather Bigard, *Treasurer*

KENTUCKY STATE UNIVERSITY
INSTITUTIONAL OFFICERS

Dr. Koffi C. Akakpo

Nineteenth President

Dr. Michael D. Dailey

Provost and Vice President for Academic and Student Affairs

Dr. Heather Bigard

Vice President for Finance and Administration / CFO

Mr. Michael R. DeCourcy

Vice President for External Relations and Institutional Advancement

Dr. Wendy D. Dixie

Vice President for Information Technology and Special Assistant to the President

Ms. Nicole Sergent

General Counsel

KENTUCKY STATE UNIVERSITY
BOARD OF REGENTS
SPECIAL MEETING

**** Meeting Will be Conducted in Person and videoconference ****

Tuesday, March 3, 2026
1:00 p.m. EDT

Board of Regents Room
Julian M. Carroll Academic Services Building, 2nd
Floor 400 East Main Street
Frankfort, Kentucky 40601
(Primary Physical Location)
Webinar ID: Webinar ID: [98255858454](#)

Zoom Link: <https://kysu.zoom.us/j/98255858454>

Phone one-tap: +13017158592,,98255858454# US (Washington DC)
+13052241968,,98255858454# US

- | | |
|--|---|
| 1. Call to Order | Regent Tammi Dukes
Board Chair |
| 2. Roll Call | Nicole Sergent
General Counsel and
Board Secretary |
| 3. Approval of the Agenda | Chair Dukes |
| 4. Division of Academic and Student Affairs Committee | Dr. Michael Dailey
Provost & VP of Academic
and Student Affairs |
| Online Student Identity Authentication Policy,
Online Privacy Policy (Action Items) | Dr. Tierra Freeman and
Dr. Michael Dailey |
| 5. Athletics
Approval of "Wall of Honor" at Alumni Stadium
and William Exum Center (Action Item) | Grant Stepp, Athletics Director |
| 6. Legal and Personnel Matters (Closed Session) | Chair Dukes |
| 7. Closing Remarks | Chair Dukes |
| 8. Adjournment | Chair Dukes |



KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

POLICY TITLE:

KYSU Online Student Identity Verification Policy

VOLUME, SECTION & NUMBER:

1.3.20

ENTITIES AFFECTED:

Students in online courses

ADMINISTRATIVE AUTHORITY:

Information Technology

Office of Online Education

APPROVED BY:

Information Technology

The Kentucky State University Board of Regents

EFFECTIVE DATE:

Click or tap to enter a date.

PURPOSE:

The Online Student Identity Verification Policy converges with many other policies and procedures of Information Technology Services at Kentucky State University to ensure that students who register for online courses are the same individuals who complete the course requirements for credit through academic engagement.¹

POLICY STATEMENT:

Students who register for online courses offered in the KYSU Online programs must be the same individuals who complete the requirements of their online courses, including academic engagement with faculty and classmates, course assignments, and assessments of course learning outcomes. Only registered students can access technology resources, such as the Learning Management System, and complete coursework for credit awarded to the registered student's transcript.

¹ See the Information Technology policies posted here: <https://www.kysu.edu/finance-and-administration/information-technology/policies-procedures.php>



KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

Admitted students are assigned a Kentucky State University email account, which they will use to access the technology resources and Learning Management System housing their online courses and learning resources. The Kentucky State University account is part of the kysu.edu domain and conforms to the security protocols of KSU's Information Technology Services.²

Students must abide by the Information Technology policies and procedures for acquiring a KSU computing account, securing it, authenticating their access to it, and securely accessing the data, educational content, and technology resources of Kentucky State University.

PROCEDURES:

When students enroll at Kentucky State University, they are assigned a University computing account on the kysu.edu domain.³ This account is associated with their KSU ID, which the Registrar assigns. After students log in to their University account, they must create a password that resets every 180 days, conforming to the following criteria:

- Passwords must be at least 12 characters in length.
- Passwords must contain at least:
 - One (1) UPPER-CASE alphabet character
 - One (1) lower-case alphabet character
 - One (1) special character (e.g., *, %, !, etc.) or number not containing any part of your name or username, not be a password you have used in the past two years
- Passwords expire every 180 days.⁴

In addition to this account password security, the University computing accounts require multi-factor authentication.⁵ Once students complete account set-up, they use their KSU computing account to log on to the KYSU Online learning management system to access their courses.⁶ Students can access their courses and learning resources only if their KSU computing account (on the kysu.edu domain) has been assigned to the course by the Learning Management System Administrator in coordination with the Registrar's Office and the Office of Online Education. This ensures that only students who have completed course registration as confirmed by the Registrar are granted access permissions to credit-bearing courses.

Students also use their computing accounts to access enterprise applications, such as Microsoft 365. The files created in these apps are uploaded into the Learning Management System and associated with their user ID, course, and relevant assignment for grading by the course instructor. Students are

² https://www.kysu.edu/documents/information-technology/Security_Access_Control_Policy.pdf

³ <https://www.kysu.edu/finance-and-administration/information-technology/ksu-computing-accounts.php>

⁴ <https://www.kysu.edu/finance-and-administration/information-technology/account-information-faq.php>

⁵ <https://www.kysu.edu/finance-and-administration/information-technology/two-factor-authentication.php>

⁶ <https://www.kysu.edu/finance-and-administration/information-technology/blackboard-login.php>



KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

required to use the University computing account to communicate with faculty, staff, and classmates. This involves email communication through the LMS, Microsoft Outlook, and Microsoft Teams. Likewise, the administrators, faculty, and staff communicate with students using an official email address.

- To uphold the academic conduct policies of KYSU Online, students are not permitted to enlist another individual or individuals to complete any course requirements on behalf of the student. See *1.3.6 KYSU Online Academic Code of Conduct* (excerpt below).

Academic Integrity is a fundamental value of Kentucky State University's community of students, faculty, and staff. The University wishes to promote the highest and most honorable pursuit of intellectual achievement and emphasize the importance of in acts of academic dishonesty may be subject to sanctions. Any student who knowingly assists in any form of academic dishonesty may also be subject to sanctions. Academic dishonesty can occur in several forms, some of which include cheating, plagiarism, and forgery. Each student is responsible for understanding the definitions of cheating, plagiarism, and forgery. The definitions are presented here and/or can be found in the KYSU Online Academic Code of Conduct, which describes the processes for the investigation and determination of academic dishonesty or misconduct.

Cheating is the fraudulent or deceptive taking, giving, or presenting of any information or material with the intent of aiding oneself or another on any academic work that is considered in the determination of a course grade.

Forgery is falsely recording the signature of an advisor, instructor, or any University official on any official University academic document.

Plagiarism is the intentional or unintentional act of submitting the work of another as one's own. If a student has any uncertainty regarding plagiarism in the submission of any class material, he or she should discuss the matter with the instructor prior to submission of the material.

Examples of plagiarism include: submission of the complete or partial work, or of the words, ideas, or format of another, published or unpublished, without appropriate reference and source credit; and *employing or permitting another person to produce, alter, or revise material that the student submits as his or her own work.*

- To uphold the Information Technology policies and information security protocols of Kentucky State University,⁷ students are not permitted to give others access to their University computing account.
 - The policy, *Use Of University's World Wide Web/Internet – Students*, says it is a violation for students to – “Whether by email or other Internet resources with a login account assigned to someone else. Forgery or attempted forgery of email messages is prohibited.”⁸
 - “Acceptable conduct in and use of this environment must conform to: existing University policies, guidelines, and codes of conduct; KSU's Internet, Intranet, E-mail, Intellectual

⁷ https://www.kysu.edu/documents/information-technology/Security_Policy.pdf

⁸ https://www.kysu.edu/documents/information-technology/IT-IM-07-2013_PolicyInternetForStudents_Final.pdf



KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

Property and Information Resource Policies; KSU Board of Regents policies and guidelines; the usage guidelines of other networks linked to KSU's networks or computer systems, and existing local, state, and federal laws.”⁹

- See also the policy statement, *4.3.1 Appropriate Usage (Information Technology)*.¹⁰

RELATED POLICIES/DOCUMENTS:

See the Information Technology policies listed in Volume 4 on the KSU website.¹¹

Information Security Policy¹²

Information Technology Appropriate Usage Policy¹³

Security Awareness and Training¹⁴

Access Control Policy¹⁵

Information Technology: Audit and Accountability¹⁶

Data Classification Policy¹⁷

Security Incident Response Policy and Procedure¹⁸

University Data Policy¹⁹

Use of University Electronic Mail (E-Mail)²⁰

Password Policy²¹

⁹ See the Kentucky State University policies posted here: <https://www.kysu.edu/finance-and-administration/information-technology/policies-procedures.php>

¹⁰ https://www.kysu.edu/documents/information-technology/ITIM012013_AppropriateUsePolicy_Final.pdf

¹¹ <https://www.kysu.edu/policies/volume-4-finance-administration.php>

¹² https://www.kysu.edu/documents/information-technology/Security_Policy.pdf

¹³ https://www.kysu.edu/documents/information-technology/ITIM012013_AppropriateUsePolicy_Final.pdf

¹⁴ https://www.kysu.edu/documents/information-technology/Security_Awareness-_Training_Policy.pdf

¹⁵ https://www.kysu.edu/documents/information-technology/Security_Access_Control_Policy.pdf

¹⁶ https://www.kysu.edu/documents/information-technology/Audit_and_Accountibility.pdf

¹⁷ https://www.kysu.edu/documents/information-technology/Data_Classification_Policy.pdf

¹⁸ https://www.kysu.edu/documents/information-technology/Security_Incident_Response.pdf

¹⁹ https://www.kysu.edu/documents/information-technology/IT_IM_09_2013DataPolicyFinal.pdf

²⁰ https://www.kysu.edu/documents/information-technology/IT-IM-02-2013_EMAIL_Policy_Final.pdf

²¹ <https://www.kysu.edu/documents/information-technology/IT-IM-11%20Password%20Policy%20for%20KSU%20ONE%20LOGIN%20accounts-2020.pdf>



KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

Use of the University's World Wide Web/Internet - Students²²

1.3.6 KYSU Online Academic Code of Conduct

4.3.1 Appropriate Usage (Information Technology)²³

STATUTORY OR REGULATORY REFERENCES:

The 2024 SACSCOC Principles of Accreditation, Standard 10, references the SACSCOC Distance Education Policy, which states that institutions should ensure students taking online courses are the same individuals who enrolled and registered:

"An institution that offers distance or correspondence education:

- (a) ensures that the student who registers in a distance or correspondence education course or program is the same student who participates in and completes the course or program and receives the credit.
- (b) has a written procedure for protecting the privacy of students enrolled in distance and correspondence education courses or programs.
- (c) ensures that students are notified in writing at the time of registration or enrollment of any projected additional student charges associated with verification of student identity."²⁴

The SACSCOC Distance Education and Correspondence Courses Policy Statement says the following:

"At the time of review by SACSCOC, the institution demonstrates that the student who registers in a distance or correspondence education course or program is the same student who participates in and completes the course or program and receives the credit by verifying the identity of a student who participates in class or coursework by using, at the option of the institution, methods such as (1) a secure login and password/passcode, (2) proctored examinations, and (3) new or other technologies and practices that are effective in verifying student identification (See Standard 10.6 [Distance and correspondence education])."²⁵

POLICY OWNER/INTERPRETING AUTHORITY:

The Office of Online Education

Information Technology

DOCUMENT DATE AND VERSION:

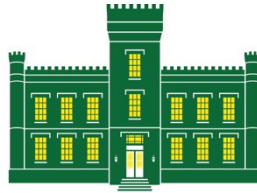
10/04/2024 – 2024.10.04_KYSU_Online Student Identity Authentication Policy_v1.docx

²² https://www.kysu.edu/documents/information-technology/IT-IM-07-2013_PolicyInternetForStudents_Final.pdf

²³ <https://www.kysu.edu/policies/files-for-volumes/appropriate-usage-4-3-1.pdf>

²⁴ <https://sacscoc.org/app/uploads/2024/01/2024PrinciplesOfAccreditation.pdf>

²⁵ <https://sacscoc.org/app/uploads/2019/07/DistanceCorrespondenceEducation.pdf>



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:

2/20/2026

NEXT REVIEW DATE:

5/1/2026

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:
