KANSAS WESLEYAN UNIVERSITY

POLICY ON VERIFICATION OF STUDENT IDENTITY

Administrative Division	**Academics**
Policy Title	**Policy on Verification of Student Identity**
Administrative Office	**Provost's Office**
Effective Date of Policy	**April 27, 2026** **Amended: 10.26.26**

Purpose

This policy establishes procedures for verifying the identity of students enrolled in online (distance education) courses at Kansas Wesleyan University (KWU), in compliance with the Higher Learning Commission's Federal Compliance requirements and federal regulations (34 CFR §602.17(g)) which states:

> *(g) Requires institutions to have processes in place through which the institution establishes that a student who registers in any course offered via distance education or correspondence is the same student who academically engages in the course or program.*

This policy ensures that KWU maintains academic integrity while protecting student privacy.

In addition to FERPA obligations, Kansas Wesleyan University maintains safeguards consistent with the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule for 'customer information' handled in the administration of student financial services (including Title IV federal student aid and related billing/financial assistance records). Records created or received under this policy may include personally identifiable information (PII) and, when related to financial aid or billing, GLBA-covered customer information. Such information must be collected, used, shared, retained, and disposed of in accordance with the University's Information Systems Program, data classification standard, and incident response procedures.

Policy

KWU is committed to verifying that the student who registers for an online course is the same student who participates in, completes, and receives academic credit for the course. KWU also ensures that all methods used for identity verification uphold the highest standards of student privacy and data security.

Procedures

Identity Verification Methods

KWU employs the following methods to verify student identity for admission to online programs:

Applicants to online programs must submit a copy of a valid government-issued photo ID to the Admissions Office. The applicant must also complete a video call with a university representative to verify their identity.

Identity verification must be completed before an online student may enroll in classes. If the required identification is missing, the applicant cannot be matched to the identification, or staff have other concerns, the applicant's status may be placed on hold or the application may be terminated.

KWU employs the following methods to verify student identity in online courses:

1. **Secure Login and Password (Primary Method)**
    - All students are issued unique KWU credentials (username and password) upon enrollment.
    - Multi-factor Authentication (MFA)
    - Access to Canvas, KWU's official learning management system, requires authentication through these credentials.
    - Students are responsible for maintaining the confidentiality of their login information.
2. **Integrated Identity Verification Tools (Supplemental Methods)**
    - Canvas supports integration with third-party tools such as Respondus LockDown Browser, Proctorio, & Proctor U for secure online testing environments.
    - These tools may include webcam monitoring, ID verification, and keystroke analysis during assessments.
3. **Instructor Verification Practices**
    - Faculty may use personalized assignments, discussion boards, and synchronous video sessions (e.g., Microsoft Teams ©) to confirm student identity through engagement and participation.
    - Instructors are encouraged to design assignments and assessments that reflect individual student learning and discourage impersonation.

Privacy Protection Measures

KWU ensures that all identity verification methods are compliant with the Family Educational Rights and Privacy Act (FERPA) and institutional data protection policies:

- Student credentials are stored securely and managed by KWU's I.S. department using encrypted systems.
- Third-party tools used for identity verification are vetted for FERPA compliance and data security standards.
- Students are informed of any additional identity verification requirements at the time of course registration or syllabus distribution.
- No biometric data or personally identifiable information is collected without explicit consent.

Record Retention, Disposal, and Incident Reporting

Retention and Disposal: Records are retained only for the period required by policy, law, accreditation, or legitimate institutional need, then securely destroyed. Paper records must be cross-cut shredded or disposed via approved secure destruction services. Electronic records must be deleted or sanitized using University-approved methods. Incident Reporting: Any suspected or confirmed unauthorized access,

misdirected transmission, loss of device/media, or exposure of PII/GLBA customer information must be reported immediately to Information Systems/Compliance and handled under the University's Incident Response Policy.

Third-Party Service Provider Requirements

When third-party identity verification or proctoring services are used, the University will ensure service providers maintain appropriate safeguards consistent with the University's Information Security Program and GLBA expectations, including: documented security review prior to adoption; contract terms governing data ownership, permitted use, confidentiality, encryption, subcontractor controls, retention/deletion timelines, and breach notification; and ongoing monitoring (e.g., security attestations such as SOC 2/ISO 27001 where available, or equivalent evidence). Service providers may only receive the minimum information necessary to perform the service.

Review and Compliance

This policy is reviewed annually by the Provost Office, Director of Online Learning & Educational Technology, and the Compliance and Data Integrity Committee to ensure continued compliance with federal standards and evolving best practices in online education.

Training and Adherence Requirements

KWU ensures that all employees involved in the development, delivery, or oversight of online (distance education) courses receive timely training on the procedures, privacy protections, and identity-verification requirements outlined in this policy. Training occurs during onboarding and is reinforced through annual updates, periodic compliance briefings, and targeted professional development coordinated by the Provost Office, Online Learning, Information Systems, and Compliance units.

This requirement also applies to **third-party contractors** acting on the University's behalf in any capacity related to student identity verification, proctoring, authentication systems, or technical support. Contractors are provided with appropriate orientation to institutional expectations, and their adherence is ensured through contractual obligations, compliance reviews, security attestations, and ongoing monitoring to verify alignment with FERPA, GLBA, and KWU's Information Security Program.