10.6.b

Distance and Correspondence Education: Protecting Student Privacy

An institution that offers distance or correspondence education:

b. has a written procedure for protecting the privacy of students enrolled in distance and correspondence education courses or programs.

Judgment

☑ Compliant ☐ Non-Compliant ☐ Not Applicable

Narrative

The polices and procedures described below are used to protect the privacy of students enrolled in distance education courses on both the Columbia and the regional Palmetto College campuses.

Initial Verification and Privacy

The University of South Columbia utilizes the same University of South Carolina system-wide login and pass-code security system for all students, including those enrolled in distance education (distributed learning) programs or courses. The initial verification of identify of students enrolled in distance education (distributed learning) courses follows the same process as that of student enrolled in on-campus courses. As such, the University applies the same privacy policies for distance education students as it does traditional, face-to-face students. (The University of South Carolina Columbia does not offer correspondence courses.)

Written procedures are distributed by the Office of the Registrar and are consistent with the Family Educational Rights and Privacy Act (FERPA), a federal privacy law that gives students certain protections with regard to their education records, such as grades, transcripts, disciplinary records, contact and family information, and class schedules. The University of South Carolina Columbia has written procedures for protecting the privacy of students enrolled in distance education courses or programs. The University complies with FERPA, the South Carolina Family Privacy Protection Act of 2002 (SC Code of Laws 30-2), and the following policies and procedures to ensure student record confidentiality:

ACAF 3.03 Handling of Student Records

Describes how the University of South Carolina collects personal student information considered necessary to fulfill its purpose as an institution of higher education. Describes how the information is maintained and made available in accordance with the federal Family Educational Rights and Privacy Act (FERPA), and the South Carolina Family Privacy Protection Act of 2002.

UNIV 1.51 Data and Information Governance

The University of South Carolina System (USC) acknowledges that its data and information are vital and valuable assets and is committed to establishing governance programs that ensure the appropriate use, availability, and risk mitigation for data and information assets. This policy describes how data and information governance programs are developed, implemented, and maintained for the benefit of the University of South Carolina system and its Constituents.

UNIV 1.52 Responsible Use of Data, Technology, and User Credentials

Outlines the requirement for all individuals and organizational units that use or access university data, technology, and user credentials to: comply with state and federal laws, statutes, and regulations; comply with all applicable university policies, standards, and procedures; must have prior authorization for related activities based on job duties or other demonstrated need; and not compromise the appropriate availability, confidentiality, integrity, privacy, or security of data, technology, and user credentials. In order to successfully carry out its mission, the University of South Carolina will act to protect the confidentiality, integrity, and availability of data, technology, and user credentials. The University of South Carolina promotes responsible use and prohibits unauthorized use of these university assets, including for personal or other nonuniversity purposes.

IT 3.00 Information Security

The University of South Carolina (USC) strives to provide a safe computing environment, and is committed to securing its data and information technology (IT) resources per state and federal laws, statutes, and regulations. In order to support risk management and compliance efforts, the University Information Security Office (UISO) is authorized to administer the university-wide Information Security Program. The UISO develops and publicizes the Information Security Program and coordinates all security incident response. Users and managers of university data and IT assets follow the Information Security Program. The University of South Carolina prohibits interference with–or avoidance of–security measures. Such actions may be grounds for investigation and disciplinary action.

All faculty and staff who access individual student information are required to read a FERPA tutorial and then take and pass

an online FERPA quiz before being given access to course rolls or the student database (Banner®). After passing the quiz, the individual must print out and sign the Banner Account Request Form (see below), a document certifying understanding of the law; this document is then signed by the employee's supervisor and uploaded into the DAPS System for processing. All faculty and appropriate staff must retake the quiz annually to ensure continued understanding of the law.

The University has three systems that require faculty and staff to submit account request forms documenting their understanding of privacy policies for distributed learning (distance education) students.

Internet Native Banner

Internet Native Banner is the student information system at the University of South Carolina. It is primarily used by core administrative offices including the offices of admissions, registrar, financial aid, and bursar to view and maintain data and process transactions. Faculty and Staff that need access to Banner are required to complete the Banner Account Request Form. The form includes several written references to the protection of privacy for distributed learning (distance education) students.

Cognos Datawarehouse

Cognos Datawarehouse is a repository of generated reports from student, financial, and human resource systems. Authorized student support staff can view, access, and print reports for administrative purposes. Faculty and Staff that need access to Cognos are required to complete the Cognos Access Request Form. The form also includes several written references to the protection of privacy for distributed learning (distance education) students.

DegreeWorks

Degree Works aids both students and advisors in monitoring students' progress toward their degree and assist students in choosing the most appropriate courses to fulfill degree requirements. Faculty and Staff that need access to DegreeWorks are required to complete the DegreeWorks Access Request Form. The form also includes several written references to the protection of privacy for distributed learning (distance education) students.

Upon admission to the University, students have access to policies regarding student privacy (FERPA) in the University Bulletin and on the Registrar webpage. As part of each new student orientation session, both students and their parents are presented with information on FERPA and the University of South Carolina Columbia's compliance related with policies. The Registrar website further clarifies that distance education (distributed learning) students are covered/protected by FERPA by specifically identifying distributed learning students (students taking online courses) as covered by FERPA.

Ongoing Protection of Privacy of Students Enrolled in Distance Education Programs or Courses

Some distributed learning courses use the optional online test proctoring provided by ProctorU or Respondus with whom the university is contracted. These online test proctoring services are optional and are not required by the university, nor are they required by all distance education (distributed learning) courses. If these optional third-party services are utilized by the student, their privacy is protected via provisions outlined in the contact signed by the third-party service and the University of South Carolina. If the third-party services are not utilized, then the distance education (distributed learning) student undergoes no additional verification of identify and is not also required for students enrolled in on-campus courses and described in the above section.

Proctor U

The University's contract with ProctorU includes a FERPA disclosure statement in which the University agrees ProctorU is an authorized agent of the Institution for purposes of receiving, storing and distributing personally identifiable information (PII) and education record protected under the U.S. Family Educational Rights and Privacy Act (FERPA). ProctorU agrees it will collect and store data including an examinee's name, address, email address, phone number and institution of enrollment when the examinee creates a ProctorU online user account, user ID and password. By creating such an account, an examinee agrees to the ProctorU Terms of Service and Privacy Policy which allow ProctorU to take the examinee's directory-based data and record the examinee in the event of a breach of procedure. During the exam process, ProctorU may make notes regarding the examinee's recorded behavior. Such notes will be stored with the examinee's directory information. All data will be stored on a secure service only accessible via password. The University will provide a list of designated users who have an authorized purpose for accessing the data and ProctorU will provide those users with access based on a username and password. ProctorU will not provide access to unauthorized personnel or any third party and will promptly notify the institution of any unintended disclosures.

Respondus

The University's contract with Respondus includes a privacy and security policy that states that Respondus Monitor uses industry standard Secure Sockets Layer or Transport Layer Security encryption to transfer information. Respondus Monitor sessions can only be recorded and accessed through Blackboard and only users with instructor credentials for the course are able to view the video sessions. In addition, video URLs are one-time use and will not function if copied.

Sources

ACAF 3.03 Handling of Student Records

- Banner Access and Confidentiality Form
- Cognos Data Access Agreement
- DAPS System
- DegreeWorks Access request
- FERPA Quiz
- FERPA Tutorial
- IT 3.00 Information Security
- ProctorU Contract
- ProctorU Contract (Page 8)
- RESPONDUS Monitor Contract
- RESPONDUS Monitor Contract (Page 1)
- Registrar - FERPA Privacy
- Registrar - Privacy
- SC Code of Laws - Title 30 - Chapter 2 - Family And Personal Identifying Information Privacy Protection
- UNIV 1.51 Data and Information Governance
- UNIV 1.52 Responsible Use of Data, Technology, and User Credentials
- University Bulletin - FERPA