REGIS UNIVERSITY

OFFICE OF FINANCIAL AID

11/01/2022

Re: GLBA Compliance - Ensure the Security and Confidentiality of Customer Financial Information

The Office of Financial Aid and Regis University are required and committed to ensuring the security and confidentiality of customer (prospective students, students, staff, faculty, and alumni) financial information.

Beyond GLBA, Regis agrees through the General Terms and Conditions of the Federal Program Participation Agreement to comply with Section 3:

c. The Family Educational Rights and Privacy Act of 1974 and the implementing regulations, 34 C.F.R. Part 99;
f. The Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm-Leach-Bliley (GLB) Act, P.L. 106-102. These Standards are intended to ensure the security and confidentiality of customer records and information. The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability as stated in 34 C.F.R. § 668.16(c). Institutions are strongly encouraged to inform its students of any such breaches. Institutions are required, pursuant to the Student Aid Internet Gateway (SAIG) Agreement, to notify the Department of any suspected data breaches.

The Student Aid Internet Gateway (SAIG) Agreement requires that any staff designated as Primary or Non-Primary Destination Point Administrators agree to the following:

- Must ensure that SAIG computing resources are used only for official government business.
- Must ensure that a substantially established relationship with the applicant is in place (e.g., the applicant has applied for admission to the institution, the applicant has included the institution on the FAFSA, the Lender holds a loan for the borrower, or the applicant applied for a loan with the Lender) before accessing Federal Student Aid systems to obtain privacy protected information about the student.
- Must maintain a profile within the EDconnect software, unless the organization uses TDClient. (See the EDconnect Help Text for instructions on how to create and maintain these profiles. See Attachment B of the SAIG Enrollment Form for the User Statement.)
- Only the DPA listed in Step One, Question 4, page 13 and referenced in Question 12, page 18; Question 17, page 20; Question 18, page 21; and Question 20, page 22 is permitted to use the National Student Loan Data System (NSLDS).
- Must use software provided by the Department to monitor SAIG mailbox activity. This software will keep track of who is using the Destination Point (TG Number/Mailbox), what information is being used, the date and time, and the batch number (if applicable).
- By applying for access to Federal Student Aid systems, must consent to monitoring, recording, and auditing, and acknowledge that information gained in this manner may be disclosed by the Department to an appropriate third-party (e.g., law enforcement personnel).

- Must ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel. In the event of an unauthorized disclosure or breach of applicant information or other sensitive information (such as personally identifiable information), the DPA must notify Federal Student Aid immediately.
- Must ensure that password sharing, the sharing of system access, and the use of any tools that allow access to FSA systems is strictly prohibited. (These tools are called "authenticators.")
- Must ensure that access is provided only to systems, networks, data, control information, and software for which the DPA is authorized.
- Must ensure that procedures for sanitizing stored information are followed (e.g., overwriting disks that contain sensitive information before reuse).
- The Non-Primary DPA must inform the organizations Primary DPA when access to a Federal Student Aid system is no longer required (i.e. the individual is leaving a position or his or her job responsibilities have changed).

Additional Requirements of the Primary DPA:

- Must ensure that all users, whether DPAs or other authorized users, are aware of and are in compliance with all of the requirements of a DPA.
- As required for eligibility to access Federal student Aid Systems, the Primary DPA must validate the individuals enrolled for SAIG Mailbox and online services for your organization on a schedule determined by ED. If validation is not completed via the SAIG Enrollment Web site within the prescribed timeframe, all services assigned to the organization and individuals could be permanently deactivated.
- Must maintain copies of all SAIG enrollment documents submitted to the Department, including the signed "Responsibilities of the Primary and Non-Primary Destination Point Administrator" form for all DPA's and the certification signed by the organization's CEO.

Additionally, the Office of Financial Aid (OFA) reviews when on-boarding new OFA staff and student employees and then annually the confidentiality expectations and requirements for all information security, not just financial.