nōssi®
COLLEGE *of*
ART & DESIGN
nashville | nossi.edu

Safeguarding Student Privacy 2023 - 2024

Safeguarding Student Privacy

Information Security Policy and Procedure

Nossi College of Art & Design is committed to maintaining reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of federal student aid information, including the safeguards required by the Federal Trade Commission Standards for Safeguarding Customer Information (16 CFR Part 314) and by FERPA (20 U.S.C. § 1232g, 34 CFR Part 99).

All student financial aid records are collected, accessed, processed, used, transmitted, stored, and disposed of by the Senior Financial Aid Officer. Access to this information is restricted to the Financial Aid Office and other authorized personnel or as requested by independent auditors during annual reviews to ensure compliance with federal, state, and institutional policies. All student financial aid files are kept on-site in a locking cabinet within a locked room with access by authorized personnel only. All electronic records are kept on secure private remote servers or in an on-site locked server room with access by authorized personnel only. Service providers for financial aid records are limited to the U.S. Department of Education's software programs of ED Connect, ED Express, NSLDS, and COD. The secure disposition of the shredding of paper records is handled by authorized personnel only.

Additional information can be found in the Financial Aid Policies and Procedures Manual. CYBERSECURITY AND THE GRAMM-LEACH-BLILEY ACT (GLBA) As a post-secondary educational institution entrusted with student financial aid information, Nossi College of Art continues to develop ways to address cybersecurity threats and to strengthen our cybersecurity infrastructure. Under the U.S. Department of Education's Program Participation Agreement and the Gramm-Leach-Bliley Act (GLBA) (15 U.S. Code § 6801), Nossi College of Art protects student financial aid information, with particular attention to information provided to Nossi College by the U.S. Department of Education or otherwise obtained in support of the administration of the Title IV Federal student financial aid programs. This includes, but is not limited to, developing, implementing, and maintaining a security program, limiting access to authorized users, and conducting risk assessments.

The Information Technology (IT) Manager oversees Nossi's cybersecurity program with limited access by other authorized personnel as needed. Nossi's IDENTITY THEFT PREVENTION strives to ensure compliance with the Fair and Accurate Credit Transaction Act, 15 USC. §1601 et seq. and the Federal Trade Commission's rules regarding Identity Theft (the "Red Flag Rules"). Any questions should be referred to the President/CEO. Printed copies of this policy or Nossi's Identity Theft Prevention are available upon request and can be obtained at the Front Desk, Financial Aid Office, or the Vice President for Academic Affairs Office.

Reporting a Breach to the FSA

In the event of a data breach requiring the college to report to the FSA, the following procedure applies:

An email sent to FSAschoolCyberSafety@ed.gov, cpssaig@ed.gov and copied to the President/CEO, the Department Director, the School IT manager. The President/CEO and/or IT manager has authority to contact the Education Security Operations Center at 202-245-6550 24 hours/day.

INCLUDE THE FOLLOWING INFORMATION

- Date of breach (suspected or known)
- Impact of breach (# of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information Security Program Point of Contact (email and phone)
- Remediation Status (complete, in process – with detail)
- Next steps (as needed)

The school shall report to FSA as they discover the breach so that FSA can work collaboratively with the PSI to resolve the incident

Reporting a Breach to the Students, Staff, and Faculty

In the event of a data breach, the college will email via .edu addresses, the appropriate individuals impacted from the breach. The following will be included in the email:

- Date of breach (suspected or known)
- Impact of breach (# of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information Security Program Point of Contact (email and phone)
- Remediation Status (complete, in process – with detail)
- Next steps (as needed)