2017

Policy and Procedure for Distance and/or Online Student Verification of Identity

The University of Scranton complies with the Middle States Commission of Higher Education (MSCHE) and United States Federal Higher Education Opportunity Act (HEOA) regulations regarding policies and procedures to ensure student identity verification in distance education.

<u>Identity Management</u>

Upon admission, each University of Scranton student is assigned a unique   Students are
                                                                                                        University's Strong Passwords Guideli

_____ when creating a password.

Students utilize their secure log in information and unique password to access the Learning Management Systems (LMS) and other content contained in the University of Scranton portal. Furthermore, seducational experience in person, faculty are encouraged to verify their identity via a   photographic ID.

<u>Information Security</u>

It is the student's responsibility for maintaining the security of user names, passwords, and any other access credentials assigned to them. This information may not be shared or given to anyone other than the person to whom they were assigned. Students are responsible for any use and activity of their account. Attempting to discover another user's password or attempts to gain unauthorized access to another person's files or email is prohibited. Students are also responsible for knowing and abiding by the information contained within the Student Handbook, the Academic Code of Honesty, as well as other Information Technology Policies. Failure to read university guidelines, requirements and regulations will not exempt users from

Proposed MSCHE Compliance Report Working Group October 2017
Draft Reviewed PCAPC November 2, 2017
Revised, Reviewed PCAPC November 30, 2017
Approved PCPAPC November 30, 2017

All sensitive data, including FERPA-governed and enrollment related records, are presented to students via encrypted transport methods, predominantly HTTPS. Access to such information requires valid credentials, in addition to authorization controls within the portal and LMS.

Costs

The University does not currently charge students to verify their identity, however, if a charge for student identification verification is implemented, students would be notified in writing at the time of registration.

Privacy

The University of Scranton is committed to maintaining the highest standards in ethics and compliance. Departments abide by the University Privacy and Confidentiality Policy, which guides practices to protect the privacy and confidentiality of students.

Personally identifiable information is collected by the University and may be used as the basis for identity verification at its discretion. For example, a student may be asked to provide unique information that could be compared to data in the University's records, such as date of birth, phone number, street address, student Royal Identification number or other bio-demographic information, when requesting to have his/her password reset.

The University of Scranton recognizes the privacy rights of individuals who are or who have been students, as guaranteed by the Family Educational Rights and Privacy Act (FERPA) of 1974. No information from records, files, or data directly related to a student shall be disclosed to individuals or agencies outside the University without the express written consent of the student unless otherwise permitted or required by law. The Student Rights and Confidentiality of Information policy details student's rights and University disclosure practices.

Policy Contact: The Office of the Registrar and Academic Services at 570-941-7721, or via email: registrar@scranton.edu

For questions regarding the technical procedures described in this document, or for technical support, contact the Division of Information Technology at 570-941-4357 or techsupport@scranton.edu

Proposed MSCHE Compliance Report Working Group October 2017
Draft Reviewed PCAPC November 2, 2017
Revised, Reviewed PCAPC November 30, 2017
Approved PCPAPC November 30, 2017