The University of Scranton

Acceptable Use Policy

I. Policy Statement

The University of Scranton community is encouraged to make innovative and creative use of information technologies primarily for purposes related to the University's mission, including teaching, research, scholarly pursuits, services, and business activities. That use has limitations however. This policy is designed to serve as a general guide for the acceptable use of computer and information systems and networks provided by The University of Scranton. All students, faculty, staff, and other authorized users should interpret this policy as a launch point to the various specific policies it encompasses – not as a replacement or amendment to any single one of them.

II. Reason for Policy

The University expects all members of its community to uphold the highest societal standards of respect for policy, law, the University, the community, and for all other persons.
This expectation certainly extends to include our use of computing and network resources. While there are various policies already in place to outline specific and targeted expectations, this Acceptable Use policy is designed to unite and relate these policies within the larger framework of our mission, vision, and Jesuit tradition.

III. Entities Affected by this Policy

All users of University information technology resources are governed by this policy.

IV. Web Address of this Policy

http://matrix.scranton.edu/TBD

V. Related Documents, Forms and Tools

Related documents include but are not limited to:

Information Classification & Protection Policy
(http://www.scranton.edu/pir/planning/Policy%20Files/Info%20Classification%20Policy%20Final%2004-01-11.pdf)

This policy defines how University information is classified and how it is to be protected. Students, faculty, staff, and alumni trust that the University protects their personal information as it exists in any medium — electronic, as well as all forms of paper record. This policy also helps to fulfill the requirements of federal and state information security regulations; specific examples of these regulations can be found on page 2.

Information Access Policy

Information Access Policy
(http://www.scranton.edu/pir/documents/Info%20Access%20Policy%2010-07-11.pdf)

This policy establishes the basic use and protection of all information, in any form, which is generated by, owned by or otherwise in the possession of the University, including all administrative and academic data (research data are excluded from this policy).
Note: Access University systems is subject to all federal, state, local and University policy and regulations.

Copyright Compliance and Peer-toPeer File Sharing Policy
(https://royaldrive.scranton.edu/xythoswfs/webui/_xy-23214719_1-t_oufnx4im)

The University of Scranton fully complies with copyright laws and regulations, and regulates the
use of peer-to-peer (P2P) file sharing activities on its network, which can be illegal.

Incidental Use Policy
(http://www.scranton.edu/pir/documents/Incidental%20Use%20Policy%20Final_3_20_2012.pdf)

Computers, network systems, and other technologies offer powerful tools for creating, communicating, and managing data, and for a host of other activities. Students and other groups providing sources of funding that support information technology resources at the University expect that these assets will be used in support of the University's mission of research and creative activity, teaching and learning, and civic engagement.

University Privacy and Confidentiality Policy
(https://royaldrive.scranton.edu/Groups/Planningandinformationsystems/PAIRO/Governance/Policy%20Analysis/Technology%20Policies/Policies/Privacy%20and%20Confidentiality/University%20Privacy_and_Confidentiality%20FINAL%2005-17-12.pdf?ticket=t_hC9B4uyL)

This policy establishes the principles to guide the practices of divisions and units in protecting the privacy and confidentiality of the information entrusted to us. This policy also helps to fulfill the requirements of federal and state information security regulations; specific examples of these can be found in Section V.

Student Code of Conduct
(http://catalog.scranton.edu/content.php?catoid=23&navoid=1894)

Student Handbook
Scranton.edu/handbook

Copyright Policy
(http://www.scranton.edu/academics/provost/research/pdf/Copyright_Policy.pdf)

Academic Code of Honesty

(http://catalog.scranton.edu/content.php?catoid=20&navoid=1583&hl=%22ACADEMIC+CODE+OF+HONESTY%22&returnto=search#Academic_Code_of_Honesty)

Web Guidelines

(http://www.scranton.edu/marketing-communications/web-projects.html)
A guide to page creation, oversight and maintenance of our website and social media sites.

VI. Contacts

For policy clarification and interpretation, please contact the Vice President for Planning and CIO at 570-941-6185.

For legal advice and interpretation of law, please contact the Office of General Counsel at 570-941-6213.

VII. Definitions

N/A

VIII. Responsibilities

The University of Scranton computing and network resources are to be used for University-related research, instruction, learning, enrichment, dissemination of scholarly information, and administrative activities. All use of computing and network resources must be consistent with University policies and codes of conduct, and must not violate international, federal, state, or local laws. The computing and network facilities of the University are limited and must be used wisely and carefully with consideration for the needs of others.

It is an affront to the mission of the University to use electronic mail, or any other means of communication, to insult, harass or threaten any other user. It is also a serious violation to pose as another user or hide their identity on the system. The University's computing resources and operating software are the property of the University, and users must not, knowingly or unknowingly, take actions which compromise the integrity of the system or degrade its availability to others. Individuals may not share with or transfer to others their University accounts including network IDs, passwords, or other access codes that allow them to gain access to University information technology resources.

Computing and network resources offer powerful tools for communication among members of the community and of communities outside the University. When used appropriately, these tools can enhance dialog and communication. When used unlawfully or inappropriately, however, these tools can infringe on the rights of others.

The Vice-President for Planning / CIO reserves the right for final interpretations of the applicability of this policy and decisions regarding sanctions would be made in consultation with existing governing policies and procedures.

IX. Procedures

Violations of this policy should be reported to the Vice President for Planning / CIO who will coordinate with the appropriate divisional Vice-President or designee. Violations of any part of this policy will subject violators to the regular disciplinary processes and procedures of the University that apply to students, faculty, staff, work study students, and all third parties. Depending on the individual and circumstances involved this could include the offices of Human Resources, the Provost, Student Affairs, the Office of the General Counsel, and/or appropriate law enforcement agencies.