UNIVERSITY OF BRIDGEPORT

POLICY AND PROCEDURE

TITLE:	Computer Network Acceptable Use Guidelines

POLICY STATEMENT:

University of Bridgeport is pleased to provide students access to its computing and information facilities, for the pursuit of supporting students' educational goals. Access to the University's computing facilities and networks is granted subject to Local, State, Federal laws and University Student Conduct Code. These guidelines are designed to promote legal, ethical, and academic honesty, and encourage restraint in the consumption of shared resources. Adherence to these guidelines demonstrates respect for the laws of intellectual property, ownership of data, system security mechanisms, and for an individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

PROCEDURE DETAILS:

University of Bridgeport expects students to exercise responsible, ethical behavior according to these guidelines when using its computing facilities. Access to the University Computer resources is granted as long as these guidelines are followed. By connecting and/or logging on to the University computers and networks, the user agrees to the terms and conditions of these Acceptable Use Guidelines as outlined here.

PUBLISH POLICY STATEMENT (CLICK ON BOX NEXT TO OPTION-SELECT ALL THAT APPLY):

- ☐ UNIVERSITY CATALOG
- ☐ FACULTY HANDBOOK
- ☐ STAFF HANDBOOK
- **X** STUDENT HANDBOOK

DEFINITIONS:

Commercial use of University resources

The account is intended for the pursuit of students' educational goals. Students may not use University of Bridgeport's computer resources to solicit sales, conduct business or advertise or sell a service. This also applies to the use of any University resources through their personal computer.

Copyright laws

Students may not copy or attempt to modify any University-owned software or software licensed to the University, except as permitted by the University. Any receipt, transmission, use or destruction of software or data, including peer-to-peer content, to include but not limited to music and video, must observe U.S. copyright laws, and license restrictions. Altering or destroying any document or file of which they are not the owner is a violation of these guidelines. The University reserves the right to disclose the identity of any student using a computer or to whom a computer is registered in connection with which the University receives in good faith, allegations of copyright infringement having occurred on the computer systems maintained or used by the University.

Disclaimers

The University is not responsible for any loss of data or damage to the hardware or software on their personal systems at home or in the Residence Halls. University of Bridgeport believes in the user's rights to privacy; however, when there is reasonable evident of wrongdoing, the University reserves the right to examine and impound any files, information, or computer systems attached to its networks, including email or instant messages. The University computing system and the data maintained on its network, including any University-owned or-leased work stations, belong to the University and there can be no reasonable expectation of privacy of users, including employees, in the University's property. The University reserves the right to periodically monitor or copy any data or activities on its computing system without any showing of cause are required.

Conduct which involves the use of the University resources in an inappropriate manner or which violates any person's rights may result in revocation of computing usage privileges and is subject to University disciplinary action as outlined in the University's Policies and Student Conduct Code. Such conduct may also be subject to criminal or civil legal action.

Note: All Rules and Regulations are subject to change without prior notice. University of Bridgeport reserves the right to make any changes as deemed necessary.

Misuse of the network systems

Connecting a personal computer or device to the University-owned network and computers must be authorized by University of Bridgeport's Information Technology Department. The University seeks to protect the civil, personal, and property rights of those who use its computing resources as well as those student or employment records that are maintained on its computing systems. Any unlawful attempt to access these resources is a serious offense. Students may not engage in activities that damage or disrupt hardware, software, or communications, such as virus or worm creation and propagation, or overloading the network with excessive data or requests for service.

Students may not monopolize, misuse or waste the system resources by, for example, requesting multiple copies from printers or by playing games in the labs. Students may not forge or otherwise misrepresent another's identity through any form of communication, or use the University computer systems to acquire the identification data of others by false pretense.

Also, students may not attempt to circumvent protection mechanisms or exercise security procedures in any computer or network component.

Students may not transmit or make accessible offensive, annoying, or harassing material, such as broadcasting unsolicited messages or sending unwanted mail.

Students may not intentionally access or damage systems or information that are not theirs, such as University records, or use any system for illegal activities.

Students may not use information bases, whether open or protected, to derive or generate mailing lists, either for their personal use or for anyone else.

Password and accounts

Students are responsible for account usage. Protect the password and do not tell it or show it to anyone, including family members, friends or acquaintances. Properly log out of the system when finished. Do not use another person's account regardless of how access to the account is obtained.

In the event the need arises to quickly contact the entire University community, the use of email accounts is one of the most efficient avenues the University has to disperse urgent, as well as routine, information throughout the community. Every institution of higher education or other large or complex United States organization has, in recent years, recognized that prudent risk management must address the existence of potential health emergencies, such

as infectious diseases, like Swine Flu, Sever Acute Respiratory Syndrome, or other community-wide safety concerns, mandating a mechanism be adopted that permits the rapid and widespread dissemination of bulletins across the entire campus. Accordingly, the University will assign an email account designation to each enrolled student, which must be maintained throughout the term of the student's enrollment.

EXCLUSIONS:
N/A

OFFICES DIRECTLY AFFECTED BY THE POLICY:
ACTS, Student Affairs

HISTORY:
Revised April 2025

EFFECTIVE DATE:	Unknown
RESPONSIBLE OFFICE (ONLY ONE):	ACTS
REVIEW DATE:	April 2025

APPENDIX:
NA