POLICY 8100

USE OF COLLEGE COMPUTER RESOURCES

Policy Category: Information Technology
Area of Administrative Responsibility: Information Technology Services
Board of Trustees Approval Date: April 17, 2018
Effective Date: April 18, 2018
Amendment History: N/A

Contents:

PURPOSE

Nassau Community College (the College) is committed to academic excellence and providing the resources necessary to maintain academic excellence. Pursuant to this goal, computers, computer accounts, network, wireless, Internet access, electronic mail, mobile devices, and related services (individually and collectively, these computing resources and services are referred to as the "computer system") may be provided for use by members of the College community. Access to and use of the College's computer system must be consistent with the terms of this policy, and with the goals, standards, and overall mission of the College.

SCOPE

This policy applies to any student, faculty member, staff member, employee, or other individual who has received appropriate authorization to use the College's computer system.

DEFINITIONS

Electronic Communications: All messages, data, files, programs, Internet web sites, and other material or information (individually and collectively) stored in or transmitted via the College's computer system are College records.

POLICY

A. Access to Electronic Communications:

The College reserves the right to access and disclose the content of electronic communications stored in or transmitted via its computer system as follows:

1. as deemed appropriate by Information Technology Services (ITS) Management for the administration and maintenance of the computer system;
2. when the College determines that such access or disclosure is necessary to investigate a possible breach of security, misuse of College resources, violation of law, or violation of College policies and procedures;
3. when the College determines that such access and disclosure is necessary in connection with an academic, disciplinary, or administrative inquiry, or legal proceeding; or
4. for all other purposes permitted by law.

The College may routinely monitor and log usage data such as network session connection times and end-points, computer and disk utilization for each user, security audit trails, network loading, etc.

B. Acceptable Use:

The College's computer system is provided for the purpose of supporting the educational mission and business functions of the College. All computer system users are expected to use the computer system for purposes consistent with the educational mission and business functions of the College. The College administration has sole authority to determine what uses are acceptable and which uses are inconsistent with this policy or other applicable standards of conduct.

C. Unauthorized Use:

1. **Unauthorized Activities**

Users may not engage in wasteful and/or illegal practices with respect to the College's computers or networks. These practices include, but are not limited to, the following:

a. **Game Playing -** While limited game playing and game playing that is part of a class or academic program are permitted, users are not allowed to engage in recreational or competitive game playing which utilize College computing and network resources.

b. **Viruses** – Users are not allowed to create or knowingly distribute viruses to other users, or propagate viruses through the NCC network or Internet.

c. **Chain and Hoax Letters** – Under no circumstances will users distribute chain or hoax e-mails.

d. **Unauthorized Servers** – The establishment of a background application which services incoming requests from other users for the purpose of gaming, chatting, browsing the web or transferring files is prohibited.

e. **Unauthorized Monitoring** – A user may not use computing resource to monitor or capture any electronic communication.

f. **Spamming or Flooding** – The use of NCC's e-mail system to send out unsolicited and/or unauthorized mail, or multiple mail messages to list servers or newsgroups with the intent of reaching as many people as possible is strictly prohibited.

g. **Private Commercial Business** – Computing resources will not be used for personal or private commercial business or for financial gain.

h. **Political Advertising or Campaigning** – NCC's computing resources cannot be used for any type of political advertising or campaigning.

i. **Repair or Move Computers** – Users may not attempt to repair or move any computer, network device or peripheral without proper authorization.

j. **Circumventing Security Measures** – Users are prohibited from circumventing or attempting to circumvent any system or computing security measures. This includes any software or hardware device, which intercepts or decodes passwords or similar access control information.

k. **Unauthorized Access** – Users are not permitted to use computing resources to gain unauthorized access to remote computers or to impair or damage the operation of NCC's computers, network or peripherals. This includes blocking communication lines, intercepting communications, and running, installing or sharing virus programs. Users must not use alternative methods of accessing NCC network resources, such as through dial-up or VPN unless specifically authorized by ITS Management.

l. **Network Device Installation** – Users must not implement any network device without proper authorization. This includes, but is not limited to, hubs, switches, routers, firewalls and wireless access points.

2. **Academic Dishonesty**

Practicing any form of dishonesty through use of College's computing facilities, for example cheating, plagiarism, or fraud, is prohibited.

3. **Harassment**

Using computers or networks to harass, abuse, bully, cyber-stalk or intimidate another person is prohibited. Users shall not develop or employ programs that harass other users. Users shall be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds or messages that could create an atmosphere of discomfort or harassment for others.

4. **Obscenity**

Obscene language in electronic mail, messages, process names, file names, file data, and other publicly visible forms is prohibited.

5. **Pornography**

Pornography in electronic mail, file data, web sites, and other publicly visible forms, is prohibited. Federal Child Pornography Laws makes it illegal to create, possess, or

distribute graphic depiction of minors engaged in sexual activity, including computer graphics. Computers storing such information can be seized by law enforcement authorities as evidence and the College will cooperate in investigating such activities.

Copyright Material:

The Higher Education Opportunity Act of 2008 (HEOA) requires the College to address unauthorized distribution of copyrighted materials, including unauthorized peer-to-peer file sharing. In order to meet the College's obligations under this Act, the College shall disseminate the following statement to students, faculty and staff on a regular basis:

The College strictly prohibits the users of its networks from engaging in unauthorized distribution of copyrighted materials, including unauthorized peer-to-peer file sharing. Anyone who engages in such illegal file sharing is violating the United States Copyright law, and may be subject to criminal and civil penalties. Under federal law, a person found to have infringed upon a copyrighted work may be liable for actual damages and lost profits attributable to the infringement, and statutory damages of up to $150,000. The copyright owner also has the right to permanently enjoin an infringer from further infringing activities, and the infringing copies and equipment used in the infringement can be impounded and destroyed. If a copyright owner elected to bring a civil lawsuit against the copyright infringer and ultimately prevailed in the claim, the infringer may also become liable to the copyright owner for their attorney's fees and court costs. Finally, criminal penalties may be assessed against the infringer and could include jail time, depending upon the severity of the violation.

ENFORCEMENT

If the College determines a violation occurred, the user's account may be immediately suspended, or his/her privileges may be revoked.

In addition, violation of this policy will result in disciplinary action as follows:

A. Students will be subject to disciplinary charges brought under the Student Code of Conduct.

B. Employees who are part of a bargaining unit will be subject to disciplinary action brought under their respective collective bargaining agreement.

C. Employees who are not members of a bargaining unit will be subject to discipline by their supervisor.

D. Third parties who fail to abide by this policy will be dealt with as appropriate under the circumstances.