Computer Use Procedures

TO: All New River Community and Technical College Users
FROM: Dr. David J. Ayersman, Vice President and Chief Information Officer
RE: **Computer Use Procedure**
DATE: August 1, 2025

The official **Computer Use Policy** for the college is here:
https://web.newriver.edu/procedures/NR-6.2-Computer-Use-Policy.pdf

This procedure explains how we can adhere to that policy.

Procedure Statement and Purpose

New River Community and Technical College **(the College)** provides and maintains computer and network resources to support the education, research, and work of its students and employees. This procedure statement offers members of the College's educational community standardized practices and procedures intended to ensure reliable and consistent service and compliance.

The College creates user accounts for various systems to enable access to information and resources. Receiving a user account is a privilege and can be revoked if abused.

All users of the College's electronic resources are expected to act in a responsible, ethical, and legal manner. The College's computer and network resources are state-owned resources intended to support academic endeavors primarily. Users must respect the rights and privacy of other users, share the resources equitably, and follow the College's other policies as well as local, state, and federal laws relating to copyrights, privacy, security, and other statutes regarding electronic media, information, and communications.

Although the College recognizes the role of individual privacy in higher education, and every attempt is made to honor that ideal, users must be aware that any electronic communication transmitted via the College's network or any electronic file stored on a computer or storage device owned by the College, may not remain confidential and may potentially be disclosed under the provisions of the Freedom of Information Act and other state and federal laws and regulations, as well as the College's other policies and procedures.

Procedures

The following shall govern the use of the College's computer and network resources:

1. Access to computer and network resources is restricted to authorized individuals as defined by the appropriate organizational unit. Accounts and passwords, when required, are assigned to specific individuals and may not, unless properly authorized by the College, be shared with, or used by, other persons within or outside the College.

2. Actions that harass, threaten, or otherwise cause harm to individuals are prohibited. Respect for the rights of others is fundamental to ethical behavior at the College. Actions that threaten or cause damage to other individuals are violations of both the College's policies and of West Virginia and federal law. Such actions may be prosecuted through both the College's judicial process and, independently, in state or federal court.

3. Actions that impede, impair, or otherwise interfere with the activities of others are prohibited. The College's computer and network resources are shared, and misuse of these

resources can harm other users. Accordingly, the College may require users to limit or refrain from specific uses. Intentional misuse or damage to resources is prohibited.

4. Actions that download or post to the College's computers, or transport across the College's networks, material that is illegal, proprietary, or in violation of the College's contracts are prohibited.

5. Actions performed using the College's computer and network resources, regardless of any disclaimers that might be made, ultimately reflect on the entire College community. Violations of copyright, licenses, personal privacy, or publishing obscene materials or child pornography may result in civil or criminal legal actions as well as College disciplinary actions.

6. Use of computer and network resources for commercial purposes, other than College-approved business, is prohibited. Limited personal use of the College's computer and network resources for other purposes is permitted when it does not interfere with the performance of the user's job or other college responsibilities and otherwise follows this procedure. However, college-related uses take priority over personal uses when resources are inadequate to meet both demands. Further limits may be imposed upon personal use following accepted management principles.

Security and Privacy

The College uses various methods to protect the security of its computer and network resources and its users' accounts. Users, however, should be aware that the College cannot guarantee such security and privacy. Users should also be aware that any electronic communication and data utilizing College-owned computer and network resources potentially may be disclosed under provisions of the Freedom of Information Act and other College, state, and federal laws and regulations as required.

The College assigns to selected staff the responsibility for investigating alleged violations of this procedure as well as applicable College, state, and federal laws and regulations. The College may monitor electronic activities and inspect data files and communications of individuals.

Penalties and Enforcement

Violations of this procedure should be reported to the Chief Information Officer or the Help Desk. The College administration may investigate them in cooperation with the appropriate law enforcement officials.

When New River receives a report of copyright infringement, the following steps are taken:

Network usage logs are examined to identify the computer and the user:

1. The computer is suspended from Internet access.
2. The copyright holder (or agent) who initiated the claim is notified that the issue is being addressed under the guidelines of the Digital Millennium Copyright Act (DMCA).
3. The user is informed that a copyright infringement claim has been made and is asked if the copyrighted material in question has been downloaded or shared without permission.

First-Time Offenses

If the user acknowledges using the copyrighted material without permission, we:

1. Require the user to read the **Computer Use Policy and Procedure** documents and to review information about the DMCA statute and copyright regulations.
2. Require the user to submit a statement that (a) confirms the copyright infringement, (b) acknowledges violation of the Computer Use Procedure, and (c) promises not to repeat this behavior.
3. The computer user's identity is not disclosed to the claimant.
4. Deny the user's system access to the Internet for one full week.
5. Inform the claimant that the issue has been resolved.

If the user denies using the copyrighted material without permission, we:

1. Require the user to submit a statement denying the copyright infringement claim.
2. Inform the claimant that the claim has been denied.
3. Under the DMCA, the claimant may pursue a subpoena to obtain the identity of the system user and may file a lawsuit against the user.

Second-Time Offenses

If a user acknowledges a second instance of using copyrighted material without permission, we:

1. Require the user to re-read the **Computer Use Policy and Procedure** documents and to review information about the DMCA statute and copyright regulations.
2. Require the user to submit a statement that (a) confirms the second case of copyright infringement, (b) acknowledges violation of the Computer Use Policy and promises not to repeat this behavior, and (c) recognizes that any further violations may result in academic dismissal.
3. Deny the user's system access to the campus network for a period not to exceed the balance of the semester.
4. Inform the Chief Academic Officer of the actions taken.
5. Inform the claimant that the issue has been resolved.

Respectfully,

Dr. David J. Ayersman
Vice President and Chief Information Officer
New River Community and Technical College