Procedure Number: B600.00.40.01.C
Date Adopted: September 2014
Date Revised: June 2021

TECHNOLOGY ACCEPTABLE USE

PURPOSE

Rowan-Cabarrus Community College (RCCC) provides technology resources for use by any RCCC employee, student, Contractor, third party, and the general public who uses any device, whether RCCC owned or personal to connect to the RCCC network. This technology includes, but is not limited to, all college computing equipment, software, systems, networks, electronic mail, websites, wireless, cloud computing, and Internet access. These resources are the property of RCCC and are provided to the campus community to support the College's mission and institutional goals. RCCC reserves the rights to grant, restrict, or deny privileges and access to technology resources. Any use of college technology resources for illegal, inappropriate, or obscene purposes, or in support of such activities, is strictly prohibited.

RESPONSIBILITIES

- The following guidelines will be observed when accessing RCCC technology resources:
- Users are expected to use RCCC facilities in a responsible and respectful manner.
- Users must abide by all relevant laws, regulations, and contractual obligations relating to computer resources and networks.
- Users must respect the rights of other users.
- Users are prohibited from transmitting, posting, or otherwise displaying material that is threatening, obscene, harassing, or defamatory.
- Users are prohibited from accessing the Internet for personal gain or commercial purposes.
- Usage of technology resources outside of the United States is generally prohibited and exceptions must be approved prior to travel by the employee's vice president and the CIO.
- Any RCCC related data stored on external media (e.g. CD, USB stick, cloud file storage service, hard /portable /virtual drives) is considered property of the College. In the case of employee termination (voluntary or forced) of any employee, all data must be retrieved and returned to the College before the employee's last day of employment.
- Any data stored on a college owned device (e.g. desktop PC, laptop, tablet, phone, etc.) is property of RCCC and will not be returned to an employee without the approval from a Vice President/Chief and the Chief Information Officer.

Security and Proprietary Information

- Users are required to take all necessary steps to prevent unauthorized access to the RCCC network and technology.
- Users are responsible for the security of their passwords and accounts and must keep passwords confidential and are not permitted to share accounts to anyone.
- Users are responsible for logging out of all systems and accounts when they are not being used, or locking the computer when the workstation will be unattended.
- All laptops and workstations that are part of or connected to the RCCC network are secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.
- Any encryption of information must be used in compliance with any federal, state or local laws.
- The use of USB memory devices to store confidential RCCC data is strictly prohibited (including but not limited to: student data, employee data, credit card information, or any other personally identifiable information). Storage of non-confidential RCCC data on a USB memory device is permitted as long as the device is encrypted utilizing BitLocker or another acceptable encryption mechanism approved by the Chief Information Officer.

Postings by authorized users from an RCCC email address will contain the following disclaimer:

'E-mail correspondence to and from this address may be subject to the North Carolina Public Records Law and may be disclosed to third parties by an authorized state official.
(NCGS.Ch.132)'

- All computers used by authorized users that are connected to the RCCC network, whether owned by the individual or the college, must be continually running approved virus-scanning software with up-to-date virus definition tables.

Unacceptable Usage

To prevent use of technology that adversely affects the ability of others to use the resources of the College, the following examples illustrates unacceptable use of computer resources:

- Sharing personal RCCC account credentials with anyone or logging into any system for use by another person.
- Circumventing user authentication or security of any device, network, or account.
- Wastefully using network resources for non-work or non-educational related purposes, including consuming large amounts of bandwidth for prolonged periods of time.
- Displaying images, sounds, or text containing nudity, obscenity or graphic violence (unless for educational purposes).
- Accessing any website used to promote violence, intolerant, or hate content.
- Knowingly downloading or uploading a virus.
- Violation of the rights of any person or company protected by copyright, trade secret, patent, other Intellectual Property, and all similar laws or regulations.
- Any illegal activities for personal financial gain.

- The use of a component of the RCCC network or other computing asset(s) to actively engage in procuring or transmitting material that violates any RCCC procedure.
- College network port or security scanning unless prior written authorization is provided by the Chief Information Officer.
- Unauthorized modification of College computer hardware or software (e.g. adding or removing RAM, changing hard drive).
- Making fraudulent offers of products, items, or services originating from any RCCC account or otherwise made from a computer connected to the RCCC network.
- Dispersing college or student data to Rowan-Cabarrus Community College's customers, staff, or clients without authorization.
- Storage of secure/confidential RCCC data on any USB or portable storage device not owned by the College.
- Storage of RCCC data on any "cloud" or network storage device not owned or managed by the College.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's session, via any means locally or remotely.

Administrative Data

The use of administrative data is a privilege, not a right. Inappropriate use reduces the availability of administrative data for critical operations, compromises college security and network integrity, and leaves the college open to potential litigation; therefore, inappropriate use may result in the cancellation of this privilege. Users are subject to the requirements for authorization, notification, and other conditions specified in this procedure and related procedures. The college may inspect, monitor, or disclose administrative data transactions when required by and constituted by law and/or when there is substantiated reason to believe that violations of any federal, state, or local law or any violation of Rowan-Cabarrus Community College's policies or procedures have taken place.

1. **User Responsibilities**
   RCCC faculty and staff are authorized users of the college's administrative data upon approval of the appropriate Data Administrator/Custodian**. It is the responsibility of authorized users to use administrative data in a manner that maintains the confidentiality and security of administrative data.** Users are authorized to access only the specific administrative data outlined in the signed CIS User Access Form.
   a. Authorized users shall not use RCCC's administrative data access to dispense administrative data to unauthorized college employees, to external personnel, or organizations without authorization.
   b. Authorized users are required to terminate administrative data sessions when the computer is not manned by the authorized user. An authorized screensaver requiring a password on resume must be maintained and active on all college computers with CIS access.

c. Authorized users are responsible to avoid the spread of computer viruses. Personnel shall not download or install unauthorized software (software not owned or registered to the college).

2. Staff Responsibilities

a. It is the responsibility of Data Administrators to initiate new access, or Data Administrators/Custodians to change access to specific administrative data for employees by completing the CIS User Action Form (form 1.27 A); review this procedure and the agreement with each employee; have the employee sign the agreement; and forward the signed and approved agreement to ITS.
b. It is the responsibility of the Data Administrator to authorize security class creations and Data Administrators/Custodians to authorize modifications. All security class changes will be signed by the appropriate Data Administrators and submitted to ITS. (Form 1.27 C).
c. It is the responsibility of Data Administrators/Custodians to semi-annually review access to specific administrative data for employees by signing the CIS Security listing provided semi-annually by ITS; review the access listed with each employee. The signed and approved review is then submitted to ITS (form 1.27 D).
d. It is the responsibility of designated CIS Data Administrator/Custodian or designated trainer to conduct local CIS administrative data training for new CIS users. Training classes are also available via the North Carolina Community College System Office per their training schedule. Following training, the Data Administrator/Custodian is to complete CIS Access Request Form indicating training has been completed. The records of training completion are housed in the College's employee learning management portal.
e. Within one business day of non-employment status of employee(s), ITS will be notified by the appropriate Data Owner/Administrator/Custodian of said status and complete the CIS User Action Form indicating the last date of employment. This will result in the immediate cancellation of access to administrative data, and ITS will ensure immediate termination of these services.

3. Revocation of Administrative Data Privileges

Administrative data access is a privilege that may be withdrawn by a Data Owner for violation of user responsibility. Suspected violations will be confidentially reported to the appropriate Data Owner. Confirmed violations of this procedure will be addressed under Procedure 12.19 – Personnel Actions for Violation of Employment Standards.

Network Monitoring

The RCCC Information Services Department shall monitor Internet use from all computers and devices connected to any RCCC network or owned by the College including, but not limited to, Local Area Networks (LAN), Wide Area Networks (WAN), Virtual Private Network (VPN), and Wireless Networks. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days. The monitoring system has the ability to record screenshots of websites while monitoring traffic of individual use.

Compliance

Internet, e-mail and network services are privileges that may be withdrawn by the Chief Information Officer for violation of this procedure. Suspected violations will be confidentially reported to the appropriate Vice President and any action deemed necessary will be carried out under the direction of the Chief Information Officer, Chief Human Resources Officer, and/or College President.

Original (signed) procedure is on file in the
Rowan-Cabarrus Community College President's Office
Dr. Carol Spalding, President