

POLICIES OF THE
BOARD OF TRUSTEES

2.28	Use of Information Technology Resources	1 of 3
NUMBER	TITLE	PAGE

- (1) It is the responsibility of the Board of Trustees and the College President to ensure that policies and procedures are implemented to protect the security of the College’s information technology resources, which are provided to enable college personnel to fulfill their academic and administrative responsibilities. Information technology resources may include – computer hardware, software, network and system operations, email, and data handling.

- (2) As a government organization of higher education, RCCC utilizes the North Carolina Office of Information Technology Services (ITS) as its Internet Service Provider; therefore, the College is obligated to conform to the policies and standards set forth by ITS. Use of RCCC’s information technology resources shall be consistent with local, state, and federal law and in accordance with all college policies and procedures.

- (3) Access to technology resources is a privilege and can be withdrawn from individuals who fail to use it responsibly. Users of RCCC technology resources who are determined to have purposefully violated any of the information technology policies and procedures shall be subject to disciplinary action. This action may include suspension of access, discharge, dismissal, suspension, expulsion, and/or legal action.

- (4) The following policy statements provide the administrative authority to the President to ensure security (prevent compromise) of the College’s technological resources:
 - (4.1) Acceptable Uses of RCCC Technology Resources

RCCC technology resources are intended to be used for fulfilling the mission of the College and are not be used for purposes that are illegal, immoral, unethical, dishonest, damaging to the reputation of the College, inconsistent with the College mission, or which may place the College in a libel situation.

General Authority: NC Office of ITS, Policies and Standards
Approved: 02-22-05
Revised:
Editorial Changes:

2.28	Use of Information Technology Resources	2 of 3
NUMBER	TITLE	PAGE

(4.2) Identification and Authentication Using IDs and Passwords

Users of the College’s information systems must be properly identified and authenticated before being granted access. The authentication system must limit unsuccessful logon attempts and information maintained on all logon attempts to facilitate intrusion detection. Password management capabilities and procedures must be established by the College to ensure secrecy of passwords and prevent exploitations of easily guessed passwords or weaknesses arising from long-life passwords.

(4.3) Network Security

The College is required to maintain responsibility for managing risk and providing appropriate security for its network in order to protect the integrity and stability of the statewide network operated by ITS. Security measures must conform to applicable enterprise network security standards, architecture, and policies. ITS is authorized, with proper notification, to suspend network service to the College should the level of risk warrant such action.

(4.4) Virus Protection

The College must take measures to protect its computers and data networks against viruses and other destructive programs.

(4.5) IT Risk Management

The College must implement an appropriate Information Technology Risk Management Program to ensure the timely delivery of critical automated services to college personnel.

(4.6) Remote Access

The College must ensure protection of data and provide an audit trail for accountability.

(4.7) E-Mail

2.28	Use of Information Technology Resources	3 of 3
NUMBER	TITLE	PAGE

All account holders/users of electronic mail provided by RCCC are hereby informed that their correspondence on the state information system may be subject to monitoring and disclosure.

(4.8) Disaster Recovery

The College must have an appropriate Business Continuity/Disaster Recovery Plan to ensure the timely delivery of critical functions and services to its stakeholders. This program must include the identification, classification, prioritization, and mitigation processes necessary to sustain the operational continuity of critical college systems and resources.

(4.9) Wireless Communication

RCCC prohibits access to the College networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of the College or have been granted access by Information Services are approved for connectivity to RCCC’s networks. All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic.

(4.10) Data Handling Policy Statement

The College is the owner of all administrative data; individual units or departments may have stewardship responsibilities for portions of that data. The College expressly forbids the use of administrative data for anything but the conduct of college business.

Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use.