RARITAN VALLEY COMMUNITY COLLEGE

INFORMATION TECHNOLOGY RESOURCES

Definition

Information Technology (IT) Resources at RVCC include, but are not limited to, computer equipment; mobile computing devices; fixed and mobile storage devices; operating systems; software; Internet, Intranet, and Extranet systems; database systems; communication systems; and network accounts providing electronic mail, Web browsing, and file transfer protocol (FTP) services. This definition applies to all resources that are connected to, or operated on, the College's IT systems whether owned or leased by the College or by any other individual.

General Provisions

All IT Resources at RVCC are intended to be used to support the mission of the College and the services it provides. The provisions of this policy apply to all students and employees of the College and to all consultants, contractors, and other individuals performing work for the College.

Only specifically approved devices may be connected to, or operated on, the College's IT internal networks. Unsecured wireless communication devices and mechanisms are prohibited.

Authorized users of RVCC IT Resources are responsible for maintaining the security of the Resources to which they have access, and the information stored or maintained by those resources. The College does not guarantee the confidentiality of any data stored on any of its IT Resources. Access to the College's administrative database is authorized by an individual employee security profile.

The college reserves the right to perform periodic information security risk assessments to determine areas of system vulnerability and to initiate corrective action. The College also reserves the right to monitor or audit the use of IT Resources and to establish appropriate administrative procedures to ensure compliance with this policy.

Personal Use

Incidental, personal use of the College's IT Resources is acceptable; however, users are responsible for exercising good judgment regarding such personal use. Individual College departments may establish local guidelines/procedures governing personal use. Conducting business for profit or using College IT Resources for personal gain is prohibited.

Encryption

Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive College information must use appropriate encryption to ensure security and confidentiality. Only encryption methods that have been specifically approved by the College may be used.

Passwords

Authorized users of the College's IT Resources are responsible for the security of their accounts and passwords. The College reserves the right to establish and enforce password structure requirements and expiration intervals.

Antivirus Software

All computers accessing the College's computer networks, whether owned by the College or by an individual, must have currently updated antivirus software installed and operating. Computers not meeting these antivirus requirements will be denied access to the College's networks.

Unacceptable Use

The College prohibits the use of any of its IT Resources, or any activity by users of its IT Resources, that is illegal under local, state, federal, or international laws or regulations. Such uses or activities include, but are not limited to

- Violating copyright, licensing, trade secret, patent, or other intellectual property laws.
- Unauthorized acquisition, reproduction, duplication, or transmission of copyrighted or otherwise protected materials.
- Exporting software, technical information, encryption software, or other protected technology.
- Introducing malicious, illegal, or unauthorized software into any of the College's IT Resources.
- Revealing an authorized user's account information and/or password to any other individual.
- Downloading any data from the College's administrative network without appropriate authorization.
- Using the College's IT Resources to acquire or transmit material that is in violation of harassment or hostile workplace laws or regulations.

- Making fraudulent offers of products or services using any of the Colleges IT Resources.
- Breaching, or attempting to breach, any of the College's IT security systems.
- Disrupting, attempting to disrupt, or attempting any kind of unauthorized access to the College's IT Resources or systems.
- Attempting any form of harassment using the College's IT Resources
- Intercepting, or attempting to intercept, any data or communication not intended for the specific user or for the IT Resources assigned to that user.

Electronic Mail

It is the intention of the College that email correspondence is maintained in a secure environment; however, privacy cannot be guaranteed, and users of the College's email systems should not have the general expectation of privacy for messages sent or received through those systems. The College is obligated to comply with requests for legally discoverable information stored on any of its IT Resources.

The College reserves the right to establish retention periods and storage quotas for email accounts and to access users' accounts for system maintenance or for the investigation of security or abuse incidents, or potential violations of College policy.

Students and employees are expected to read their email on a regular basis. An email message from the College administration regarding College matters is considered an official notice.

Users of the College's email systems are expected to avoid the following unacceptable practices.

- Sending "junk mail" or other unwanted material to individuals or groups of individuals who did not request such material.
- Sending messages that are harassing, threatening, or obscene.
- Promotion of individual political or religious agendas, except as part of public debate.
- Libel or slander of other individuals.
- Violating another user's privacy.
- Misrepresenting the identity of the sender of a message.
- Unauthorized use or forging of email header information.
- Solicitation of email to be sent to another's email account.
- Creating or forwarding email chain letters or other pyramid schemes.
- Postings to a newsgroup from a College email address without a disclaimer stating that the opinions expressed are not necessarily those of the College.

RARITAN VALLEY COMMUNITY COLLEGE

Student Accounts

The College provides a secure access portal and email account for each registered student. The College reserves the right to establish expiration dates and regulations for the use of these accounts.

Website

Content produced for the RVCC Website must be created using the College's approved content management system. Content posted to the Website must be approved by the appropriate College administrator and become the property of the College. The College Website may not be used for commercial or personal purposes unrelated to the College.

Course Software

Only the College's approved online course management software may be used for the delivery of credit online and online-hybrid courses. Other software may be used for supplemental materials, tutorials, examinations, and for non-credit courses

Responsible Administrator – Vice President for Technology, Assessment, and Planning

Revised and reaffirmed

- September 2011

Communication – This policy is communicated to the College community in the following documents:

- College Catalog
- Faculty Handbook
- Student Handbook
- College Website