Rock Valley College

Acceptable Use of Information Technology

RVC Administrative Procedure (2:30.060)

Purpose

Rock Valley College's (RVC) technology infrastructure exists to support the organization and activities needed to fulfill the College's mission. Access to these resources is a privilege that should be exercised responsibly, ethically, and lawfully.

The purpose of this Acceptable Use of Technology Procedure is to clearly establish the College's position relating to the acceptable use of its technology and the role each member of the organization has in protecting its information resources.

Scope

This Procedure applies to all users of technology resources owned, managed, or otherwise provided by the organization. Individuals covered by this Procedure include, but are not limited to, students, all employees and service providers, guests and anyone else with access to the organization's technology and information resources and/or facilities.

Technology and information resources include all RVC College-owned, licensed, or managed hardware and software, domains, and related services and any use of the organization's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

General Guidelines

Activities related to RVC's mission take precedence over computing pursuits of a more personal or recreational nature. Personal, non-job-related use of the College's technology, except for use by students enrolled at the College, should be incidental and kept to a minimum. Any use that materially disrupts the organization's mission or its day-to-day operational activities is prohibited.

All users of RVC's technology resources, whether use is via personally owned and/or College-owned devices, must adhere to the requirements enumerated below.

All users are responsible for using RVC's technology resources in an ethical and legal manner. Further, users are responsible for learning and adequately using all features that secure, process, and/or access data.

Privacy and Property

Users have no expectation of privacy in connection with their use of Information Technology (IT) resources, except where a user's confidential information or usage is otherwise protected by federal or state law (e.g., 20 U.S.C. § 1232g ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Personal Information Protection Act ("PIPA")). The College has the discretion to monitor the use of its IT systems with or without notice to the users, consistent with federal or state laws and regulations.

The campus network is maintained and intended to further the mission of RVC and conduct the College's daily operational activities. The network is the College's property, thus all data composed and created by employees and transmitted and/or stored on the network is and will remain College property, not the private property of any individual. Exceptions to the data ownership clause described includes unique works or creations which are protected by other laws.

Data residing on personally owned workstations that are connected to the campus network is not considered to be College property, but any data created, transmitted, accessed, and/or stored on the campus network by users of these individually owned computers is subject to the same policies, procedures, guidelines, and constraints as data created, transmitted, accessed, and/or stored using College-owned devices.

Documents, email messages, and other files deleted by users may nonetheless be archived by the College, which has a right to subsequently retrieve material, except where protected by federal or state law.

Fraudulent and Illegal Use

RVC explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any of the organization's information systems, a user must not engage in any activity that is illegal under local, state, or federal law, or any RVC Board policy or procedure. As a part of this Procedure, users must not:

- Violate the rights of any individual or company involving information protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by RVC or the individual user.
- The redistribution of any software, videography or copyrighted material in electronic format is prohibited, except in the case of material which is clearly marked as being public or freely distributable or material which is covered by the "Fair Use Doctrine." The individual user shall determine whether the material is covered by the Fair Use Doctrine, and shall be liable for any infringing use. Users who redistribute software owned by or licensed to RVC

without authorization from the Department of Information Technology violate agreements with software suppliers, as well as applicable federal copyright, patent, and trade secret laws.
- Misrepresent the user's identity or affiliation.
- Attempt to corrupt the College's information system and/or network.

Malicious Activity

RVC strictly prohibits the use of its information systems for malicious activity against other users, the organization's information systems themselves, or the information assets of other parties. Users must not:

- Perpetrate, cause, or in any way enable disruption of RVC's or any other information systems or network communications by denial-of-service, the introduction of malicious programs (e.g. viruses, worms, Trojan horses) or other methods;
- Circumvent or attempt to circumvent the user authentication or security of any information system;
- Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information; or
- Create and/or use a proxy server of any kind, other than those provided by RVC, or otherwise redirect network traffic outside of normal routing; or use any type of technology designed to mask, hide, or modify their identity for nefarious activities electronically.
- Use a port scanning or network monitoring tool targeting either RVC's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of the Department of Information Technology conducting a vulnerability scan.

Harassment

All use of College IT systems must conform to all federal and state laws prohibiting workplace harassment (including, but not limited to, Title VII, Title IX, and the Illinois Human Rights Act). Harassment of other users of information technology systems can involve the sending of unsolicited, unwanted, or nonwork-related messages or files, singly or repeatedly.

Users must not post, upload, download, or display inappropriate messages, photos, images, sound files, text files, video files, newsletters, or related materials, including but not limited to those that are discriminating; harassing; sexually explicit; violent or promoting violence.

Rock Valley College

Hardware and Software

RVC provides technology resources to employees and other personnel to ensure they have a safe and reliable computing environment from which to work. Thus, those working with or accessing institutional resources need to be sure that they are operating within the secure platforms that have been vetted and reasonably secured. As such:

- RVC prohibits the use of any hardware or software on RVC-owned computers that is not (1) purchased by the College, (2) licensed for the College's use, or (3) installed, configured, tracked, and/or managed by an authorized employee.
- All employees and service providers must use approved workstations, services, or devices to access the College's data, systems, or networks. This includes storing institutional data in cloud-services that have been approved by the RVC Department of Information Technology.
- Personally owned workstations or devices that store, process, or transmit institutional confidential information must be secured with a minimum of the following:
    - a complex password,
    - up-to-date security patches,
    - working, up-to-date anti-malware protection,
    - an up-to-date web browser to access online services through https protocols,
    - and the RVC private network (VPN) software.
    - Users must not download, install, disable, remove, or uninstall software designed to provide a secure computing environment, including patches of existing software, to any institutional information system without approval of the Department of Information Technology.
- All devices must be physically secured at all times. This includes locking a workstation when not in use and not leaving an unlocked device unattended for any length of time.
- Users must not install, connect, or disconnect unauthorized network devices on the campus network. Examples of prohibited devices include a router, network switch, wireless access point, or wireless printer with Wi-Fi Direct enabled.
- Users must take appropriate security precautions with institutionally owned devices, up to and including the utilization of a loaner device from the Department of Information Technology when working remotely.
- Technology-related theft is expressly forbidden.

Messaging

The organization provides a robust communication platform for users to fulfill its mission.

- Employees and students are expected to read their campus email, and must use their campus email accounts in official communication with campus offices and campus community members, to ensure proper identification. Based on the foregoing, employees and students are considered aware of any updates that are communicated via campus official communications to campus email accounts.
- Employees must not forward rockvalleycollege.edu email accounts, or other private or restricted institutional communications, to other email service providers.
- Students are responsible for reading and responding to official information sent to their College email account.
- Users must not send unsolicited e-mail messages, including "junk mail" or other advertising material to individuals who did not specifically request such material for commercial ventures, solicitations, religious or political causes, outside organizations, or other non-job-related endeavors.

Enforcement

RVC students believed to be in violation of this procedure will be referred to the student disciplinary procedure.

Employees believed to be in violation will be referred to employee disciplinary procedures consistent with applicable College policies and contractual obligations. All other presumed violators will be handled on a case-by-case basis.

All requests for clarifications or interpretations of this procedure should be directed to the Vice President of Operations/COO.

Implemented: March 2023