COMMUNITY COLLEGE OF RHODE ISLAND

Origination:	*01/2002*
Effective:	*10/2015*
Last Approved:	*10/2015*
Last Revised:	*10/2015*
Next Review:	*09/2016*
Owner:	*Kristen Albritton: Vice Pres-Finance and Strategy*
Area:	*Information Technology*
References:	

Responsible Use of Information Technology

BACKGROUND:

The information technology resources of the Community College of Rhode Island (CCRI) are owned and maintained by the College. Use of this technology is a privilege, not a right, and users have certain responsibilities. Use of the College's information technology resources should be in conformity with the mission, goals, and values of the Community College of Rhode Island. Therefore, use of the College's technology should be supportive of its educational and research roles, as well as its values and behavioral standards.

Acceptable use of the College's information technology resources is consistent with the principle of academic freedom. As is the case with the use of all other resources and activities provided or sponsored by the College, use of the College's information technology resources is contingent upon adherence to ethical and legal behavioral expectations and compliance with policies and procedures outlined in the College's Handbooks (Student, Faculty, and Staff). Legitimate use of a computer, computer system or network, does not extend to whatever is technically possible.

Effective security is a community-wide effort involving the support and participation of all CCRI students, employees and affiliates who deal with information and/or information systems. Members of the College community are expected to become familiar with this Responsible Use of Information Technology, to act with careful consideration of its requirements, and to seek assistance whenever necessary. This policy applies anywhere on any campus and to off campus personally owned digital devices that interact with the College information systems, network and other technology resources. College supplied accounts, including but not limited to a user's college logon ID, are the property of the College and may be revoked at any time in response to violation of the Responsible Use of Information Technology. Additionally, violation of this policy can result in further discipline under the appropriate College procedures and/or by civil or criminal prosecution. Questions regarding this policy or the application of this policy to a specific situation should be referred to the Director of Information Technology.

POLICY STATEMENT:

The purpose of this policy is to outline the acceptable use of computer systems, voice, video and data networks, information and data, and other information technology resources at the Community College of Rhode Island. These rules are in place to protect students, faculty, staff and the College. Inappropriate use exposes the College to a number of risks, including but not limited to virus attacks, the compromise of network systems and services, theft of Personally Identifiable Information, and legal liability.

DEFINITIONS:

Information technology includes but is not limited to desktop computers, workstations, network servers, mainframe computers, software, digital information and voice, video and data networks, including official College pages on social networking sites.

Guidelines for General Use

1. Information technology resources are provided to support the academic and administrative goals of the Community College of Rhode Island. These resources are limited and should be used with consideration for the rights and needs of others.
2. Information distributed through the Community College of Rhode Island's information technology resources may be considered a form of publication. Users of these resources should employ appropriate language and communication methods.
3. Unless postings from a Community College of Rhode Island email address to public forums are clearly in the course of the College's academic or administrative duties, they should contain a disclaimer stating that the opinions expressed are strictly those of the poster and not necessarily those of the Community College of Rhode Island.
4. Automated forwarding of the Community College of Rhode Island email is not supported or allowed.

Unacceptable Use

The activities listed below are prohibited. The list of prohibited activities is not all inclusive; rather, it includes examples of what the College considers to be clearly inappropriate behavior and unacceptable uses of its information technology resources**.**

1. Violation of the rights of any person or company 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 the Community College of Rhode Island or the owner of the computer.
2. Unauthorized use of copyrighted material including, but not limited to, photographic images, videos, or music, and the installation of any copyrighted software for which the Community College of Rhode Island or the end user does not have an active license.
3. Introduction of malicious programs into the network or servers.
4. Unauthorized disclosure or use of an account password, or an attempt to access, or gain actual access to, an information technology resource by providing false or misleading information.
5. Use of an information technology resource to view, create, post, transmit or receive material deemed by the College obscene, unless such activity is appropriate for academic or work purposes.
6. Use of an information technology resource to threaten or vilify others.
7. Use of an information technology resource for commercial gain, product advertisement, or political activities unless expressly authorized by a senior member of the College's administration.
8. Use of an information technology resource to make fraudulent offers of products, items, or services.
9. Deliberate disruption of the College's computer systems, networks or other information technology resources.

10. Port scanning or security scanning without prior approval by the Information Technology Department.
11. Circumvention of user authentication or security of any host, network or account.
12. Use of an information technology resource to access or transmit the files or communications of other students, faculty or staff without authorization, or to provide information about, or lists of, students, faculty or staff to persons, groups, or organizations outside the College without authorization.
13. Use of an information technology resource to engage in any activity that is illegal under local, state, federal, or international law.
14. Use of an information technology resource to send unsolicited email messages such as "junk mail" or other advertising material to individuals who did not specifically request such material.
15. Use of an information technology resource such as email, telephone, paging, text messaging, instant messaging, or any other new electronic technologies that may emerge, to engage in any form of harassment in violation of College policy and/or applicable law.
16. Unauthorized use of email header information, or forgery of email header information.
17. Use of an information technology resource to create or forward "chain letters" or other "pyramid" schemes of any type.
18. No individual or group may download or distribute files to the extent that such actions are harmful/and or disruptive to IT systems and resources. CCRI reserves the right to automatically manage and restrict excessive use of College network bandwidth.
19. Use of CCRI resources and systems unrelated to the user's College position.
20. Any communication conducting, promoting or advertising a personal commercial enterprise is prohibited. Use of electronic resources is restricted to authorized purposes consistent with the College's mission.
21. Individual or department deployment of wireless networks is not allowed. Any unauthorized wireless access point found connected to the campus network will be considered a security risk and disabled.

Security and Safeguarding of Information Technology Resources

1. Authorized users are responsible for the security of their passwords and accounts. The use of individual accounts should not be shared with another user. Passwords should be changed on a routine basis.
2. All computers that are connected to the Community College network must be running virus-scanning software with a current virus database.
3. All computers that are connected to the Community College network must be up to date with all operating system updates and patches.
4. Email attachments received from unknown senders may contain viruses, email bombs, or Trojan horse codes; therefore, they should not be opened and they should be deleted.

Confidentiality

Records maintained by the College, including those in computerized form, are vital College assets. Information contained in those records, including but not limited to academic, financial, and personnel records, are considered confidential and private. Every reasonable effort will be made to limit access of such records to authorized individuals only. However, the College may be compelled to release confidential records to comply

with legal obligations.

Users of the College's information technology resources who are authorized to access confidential records must respect the privacy rights of others and use such data only for legitimate academic or administrative purposes. Users with access to confidential data must protect the accuracy, integrity, and confidentiality of that data by taking all necessary precautions and following established safeguarding procedures.

Privacy Regarding the Use of Information Technology Resources

The College employs various measures to protect the security of its information technology resources and its users' accounts. Users should be aware, however, that the College cannot guarantee such security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should be aware that their use of the College's information technology resources is not completely private. While the College does not routinely monitor individual use of its information technology resources, the normal operation and maintenance of the College's information technology resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.

The College also may specifically monitor the activity and accounts of individual users of the College's information technology resources, including but not limited to, individual login sessions and communications, without notice, when:

1. The user has voluntarily made them accessible to the public, by, for example, posting to a Web page;
2. It reasonably appears necessary to do so to protect the integrity, security, or operation of the College or other information technology resources, or to protect the College from liability or other potentially adverse consequences;
3. There is reasonable cause to believe that the user has violated, or is violating, the College Information Technology Responsible Use of Information Technology and/or policies prohibiting harassment and violent behaviors;
4. An account appears to be engaged in unusually excessive activity, as indicated by the monitoring of general activity and usage patterns;
5. It is otherwise required or permitted by law.

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate Vice President in consultation with the General Counsel, or their respective designees.

The College, at is discretion, may disclose the results of any such general or specific monitoring, including the contents and records of individual communications, to appropriate College personnel and law enforcement agencies, and may use those results in appropriate College disciplinary proceedings. Communications made by means of College information technology resources are also generally subject to court orders, valid subpoenas, or other legally enforceable discovery requests to the same extent as they would be if the same information was available as a hard copy.

Procedure for Reporting an Alleged Misuse of the

Computer Systems/Enforcement

Members of the CCRI community who believe they have witnessed or been a victim of an incident which is in violation of this policy should notify or file a complaint with appropriate college offices as follows. Students should report suspected violations to the Dean of Students. Faculty members should report suspected violations to the Vice President of Academic Affairs. Staff members should report suspected violations to the Director of Information Technology. All listed above may report the problem to the Director of Human Resources. Reports of suspected unauthorized use or misuse of CCRI information technology resources will be investigated pursuant to standard college procedures.

Information technology users who are found in violation of this policy will be subject to CCRI disciplinary processes and procedures including, but not limited to, those outlined in the Student Handbook, the CCRI Employee Handbook, and any applicable bargaining unit contracts. Privileges to use CCRI information technology resources may be revoked. Illegal acts may also subject users to prosecution by local, state, and/or federal authorities.

POLICY APPLIES TO:

This policy applies to students, faculty, staff and agents of the Community College of Rhode Island, including all personnel affiliated with third parties, and to all other users of information technology resources at the College.

RESPONSIBLE DEPARTMENT:

Information Technology

ADDITIONAL AUTHORITY:

The examples of unauthorized use of CCRI information technology resources identified above are not meant to be exhaustive. Questions regarding this policy or the application of this policy to a specific situation should be referred to the Director of Information Technology. Whenever you are in doubt regarding an issue of questionable use, it is in your best interest to resolve the issue before pursuing any questionable use of information technology resources.

RELATED POLICIES:

This policy is supplemented by all other college policies and by the policies of those networks to which CCRI is interconnected, including but not limited to OSHEAN. Applicable local, state, and federal laws also apply to information technology users at CCRI.

Attachments

No Attachments