Computer and Network Resources Use

Policy Type: Administrative
Responsible Office: Office of Technology Services, Vice President for Administration
Initial Policy Approved: 08/19/2010
Current Revision Approved: 05/04/2017

Policy Statement and Purpose

Virginia Commonwealth University provides and maintains computer and network resources to support its faculty, staff, and students in their education, research, patient care, and work activities. All individuals receiving a university computing account, or using VCU computer and network resources, are expected to comply with this *Computer and Network Resources Use* policy. All users of these resources are expected to restrict their use of VCU computer and network resources to university-related responsibilities and actions. Limited personal use of the university's computer and network resources is permitted only when it does not interfere with the performance of the user's job or other university responsibilities or other university functions and is otherwise in accordance with this policy. Use of the university's computer and network resources for an individual's business or for personal commercial purposes is not authorized. Further limits may be imposed upon personal use in accordance with accepted management principles.

All users of VCU computer and network resources are expected to act in a responsible, ethical, and legal manner. VCU computer and network resource users must respect the rights and privacy of other users, share computer and network resources equitably and follow VCU policies and local, state, and federal laws relating to copyrights, privacy, security, and other uses of computer, networks, or electronic media. University employees are specifically prohibited from using VCU computers, networks, or electronic media in contravention of Va. Code Section 2.2-2827 as detailed more fully below.

This policy sets forth the responsibilities of faculty, staff, students and system administrators when using VCU computer and network resources and the responsibilities of the VCU Chief Information Officer in enforcing it.

Noncompliance with this policy may result in disciplinary action up to and including termination for employees or expulsion for students. Suspected violations of this policy should be reported according to the policy specifics and procedures. VCU supports an environment free from retaliation. Retaliation against any person who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Policy

Individuals who will be utilizing VCU computer and network resources are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

Definitions

Authorized Individual
Within the context of this document, an authorized individual is a VCU employee, including student workers, a student or affiliate who has been granted access to VCU computer and network resources based on their relationship with VCU.

Download
Within the context of this document, download refers to the action of transferring data from one computer system, including computer systems located on the Internet, to another computer system or to another storage medium such as, but not limited to, USB drives, tablets, phones, hard disks, or CDs.

Organizational Unit
Within the context of this document, an organizational unit is a college, school, a department, or division that reports up through a cabinet member. Examples of organizational units include School of Engineering, College of Humanities and Sciences, School of Medicine, Office of Technology Services, Enrollment Services, and Facilities Management.

Personal Privacy
Within the context of this document, personal privacy refers to the ability and right for individuals to control how information about them are collected, disseminated, and used.

Post
Within the context of this document, post refers to the action of making data or files accessible through a computer or network resource. Examples of posting activities include, but are not limited to, commenting on

an online forum, providing a status update to a social media site, or placing a file on a public server for others to download.

Server

Within the context of this document a server refers to a computer system or a collection of computer systems designed to provide services that process, store, or transmit data and information for one or multiple clients; where the client maybe other computer systems or programs that are used by individual users. A server may be hosted by VCU inside of its networks, or hosted by a third party on the Internet or other external networks.

Sexually Explicit Content

As defined in Va. Code § 2.2-2827 (i) any description of or (ii) any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting sexual bestiality, a lewd exhibition of nudity, as nudity is defined in § 18.2-390, sexual excitement, sexual conduct or sadomasochistic abuse, as also defined in § 18.2-390, coprophilia, urophilia, or fetishism.

Unit Head

A unit head is the administrative employee responsible for the operations of an organizational unit. A unit head can be a dean of a school or the director of a department or division.

Use

With the context of this document, use refers to the action of generating, accessing, modifying, viewing, downloading, posting, uploading, storing, or removing information through computer and network resources.

VCU Computer and Network Resources

All information technology (IT) resources, including but not limited to wired and wireless networks, VPN's, software or applications, servers, appliances, workstations, desktops, laptops, tablets and any mobile devices, that are used by authorized individuals in the course of their university responsibilities or are purchased with funding allocated to VCU. Free and open source software or applications used by university employees for the purpose of education, research, patient care or administration that relates to the university's mission and day-to-day operations are also considered VCU computer and network resources.

VCU Helpline

The VCU Helpline is an anonymous reporting tool that enables individuals to ask questions, report policy violations, ethics concerns, as well as other regulatory concerns with the university. The VCU Helpline can be accessed anonymously at www.vcuhelpline.com, by calling 1-888-242-6022 (from the United States) or by making a collect call to 503-748-0867 and giving the name "Virginia Commonwealth University" if calling from Qatar.

Contacts

The VCU Office of Technology Services officially interprets this policy and is responsible for obtaining approval for any policy revisions. Please direct policy questions to the VCU Office of Technology Services and / or VCU Information Security Office. To contact either office with questions or concerns, please contact the VCU IT Support Center, itsc@vcu.edu or infosec@vcu.edu or call 804-828–2227.

Policy Specifics and Procedures

Prohibited uses of VCU Computer and Network Resources

VCU computer and network resources must not be used in connection with the following:

- Conduct that harasses, threatens, or otherwise causes harm to individuals in violation of university policy, or state or federal law.

- Disruption, misuse, or damaging of any university resources; interference with university operations or the work of other users, whether intentional or not.

- Attempting to improperly obtain computer privileges or resources for persons or purposes not authorized by the university.

- Downloading or saving to university computers or other storage devices, transporting across university networks, or posting externally; material that is illegal, or that violates copyright, licenses, or personal privacy.

- Accessing, downloading, printing, uploading, or storing any information, files or services having "sexually explicit content" except for bona fide, agency-approved research approved in writing by the university president or the president's delegate, in violation of Va. Code § 2.2-2827. http://law.lis.virginia.gov/vacode/2.2-2827/

- Use of computer and network resources for commercial purposes, other than university-approved business or other business in accordance with university policies.

- Use of university websites, social media sites or other communication tools for work-related purposes that do not comply with policies, guidelines and standards established by the VCU Division of University Relations.

Protection of Computer and Network Resources

- Authorized individuals using VCU computer and network resources must follow this policy and the guidance provided and/or posted by the VCU Office of Technology Services and / or VCU Information Security Office, including the published VCU Information Security Standards.

- Authorized individuals using VCU computer and network resources are expected to use reasonable and appropriate care in their use of those resources, such as exercising prudence on accessing websites and links that might contain malware harmful to VCU systems, and placing sensitive VCU systems in physically secured locations.

Access to Computer and Network Resources

- Access to VCU computer and network resources is restricted to authorized individuals and requires valid accounts and passwords.

- Sharing accounts or passwords is a significant security risk and is strictly prohibited unless properly authorized, in writing, by the VCU Information Security Office.

- VCU may take immediate action to remove an individual's access to its computer and network resources to address security threats or manage/address credible reported violations of university policy, or state or federal laws.

Security and Privacy

- VCU computer and network resources, including email are the property of the university, not the individual. The university has the authority to monitor computing activity as part of its responsibility to operate secure computer and network systems and may monitor electronic activities and inspect data files and communications of individuals when warranted pursuant to this policy. (See details in the Investigation and Resolution of Suspected Violations section below).

- The university uses various methods to protect the security of its computer and network resources and of its users' accounts. Authorized individuals should exercise sound judgment if they elect to use VCU computer and network resources to transmit or store personal information, understanding that VCU necessarily has access to all of its computer and network resources.

- Records reflecting university business stored VCU computer and network resources are public records subject to disclosure (unless subject to exclusions) under the Virginia Freedom of Information Act.

- If monitoring of computer or network use reveals evidence of a possible violation of law, such information may be provided to law enforcement agencies.

Reporting Suspected Violations

- Anyone perceiving immediate danger or threat should contact the VCU Police immediately. (804-828-1234).

- Any discovery of child pornography residing on any university computer or system must be reported immediately to the VCU Police Department. (804-828-1234).

- Anyone who suspects a violation of the *Computer and Network Resources Use* policy is expected to report the suspected violation to the office or department where the suspected violation occurs; to the VCU [Compliance] Helpline; or to the chief information officer in accordance with the VCU *Duty to Report* policy. (see FAQ #2 for contact information on Helpline).

- Reports of suspected violations should be communicated without unreasonable delay to the chief information officer and, if the suspected violation may involve a violation of law, the CIO will immediately contact the VCU Police Department. (804-828-1234).

Investigation and Resolution of Suspected Violations of VCU Policies, State or Federal Laws; Responses to Legal Orders and Demands

- The chief information officer or designee is responsible for coordinating with appropriate administrators regarding the investigation and management of reported violations of VCU policies or applicable laws, or in response to subpoenas, discovery, FOIA requests, or lawful court orders that require access to computer or network resources. Such investigations or access may require monitoring, recording and analysis of computer activities, examination of email, network, computer and Internet usage, and files stored on a computer, and transmittal of required records to those lawfully authorized to receive them.

- A request to investigate or monitor an individual's computer or network resources must be directed to the VCU chief information officer or designee who will consult with the responsible senior administrator for the relevant unit (VP) and the Office of University Counsel. Unauthorized monitoring is prohibited and is itself considered a violation of this policy. Monitoring or other investigation necessary to protect VCU's systems may be initiated on an emergency basis at the discretion of the VCU chief information officer.

- Individuals who use VCU computer or network resources in violation of this policy or applicable state or federal laws face disciplinary actions and/or personal liabilities including but not limited to civil or criminal sanctions, fines, or other remedies that might be imposed by a court or agency.

Immediate Action Pending Investigation

- In certain circumstances, a unit head or designee may be authorized or required to take the following specific actions to either protect the university's computer and network resources or to protect the university from adverse publicity or legal liability.

- **Risk of damage to computer and network resources:** If serious risk of damage to the university's computer and network resources is present, the unit head or designee may suspend the suspected violator's access to computer and network resources and must immediately notify the chief information officer for appropriate investigation and resolution.

- **Suspected copyright or license violation:** If an individual has reasonable cause to believe that any document or file residing on or being distributed from a university system may infringe copyright or licensing responsibilities, the individual should report such concerns to the unit head or designee without unreasonable delay. If the concerns are validated, the unit head or designee should contact the chief information security officer (or designee) and, if applicable, the Office of University Counsel for guidance in addressing such suspected incidents without unreasonable delay.

Forms

There are no forms associated with this policy.

Related Documents and Reporting Systems

1. Restrictions on state employee access to information infrastructure, VA Code §2.2-2827
2. VCU Information Security Standards
3. Virginia Freedom of Information Act, VA Code §2.2-3700
4. VCU Policy: *Duty to Report*
5. VCU Policy: *Information Security*
6. VCU Policy: *Student Code of Conduct*
7. State employee use of electronic communications and social media
8. VCU Affiliate User Guide
9. VCU Code of Conduct
10. Virginia Department of Human Resource Management Employee Standards of Conduct
11. VCU Police Online Crime Reporting System
12. VCU Helpline Online Reporting System
13. VCU Information Security Incident Reporting Page
14. VCU University Relations Website

Revision History

This policy supersedes the following archived policies:

Revised 8/19/2010	*Computer and Network Resource Usage Policy*
Revised 10/12/2016	*Computer and Network Resources Use - Interim*

FAQ

1. **If I observed a violation to this policy, to whom should I report the violation?**

   In accordance with the VCU *Duty to Report* policy, an employee, affiliate or student can typically report the violation to his or her department / unit administrator or head. Alternatively, the individual can also report the violation to the VCU chief information officer or the VCU Helpline. The department or unit administrator must report the violation to the university chief information officer.

2. **Can I report a violation anonymously?**

   Yes. Questions or concerns may be submitted to the VCU Helpline anonymously at www.vcuhelpline.com, by calling 1-888-242-6022 (from the United States) or by making a collect call to 503-748-0867 and giving the name "Virginia Commonwealth University" if calling from the Qatar campus.

3. **I am a departmental supervisor and I suspect that an employee in my department is violating this policy, can I initiate monitoring on this employee's computer?**

   No. You must contact the chief information officer to report your concerns and suggest initiation of monitoring or investigation. Unauthorized monitoring is prohibited and is considered a violation of this policy.

4. **I am a VCU employee, student or affiliated personnel, can the university monitor my computer usage?**

   Yes. The university has the authority to monitor computer, network, email and Internet usage on the university network, as well as usage of university owned computers and applications on and off the university network to ensure network and information security, comply with legal requests and ensure the safety and security of the university population. Further, records of university computer and network usage data may be subject to the Virginia Freedom of Information Act. However, any monitoring of computer and network usage must be authorized by appropriate personnel and conducted by designated university staff as defined in this policy.

5. **I occasionally use the computer in my office to visit news sites and social media sites during my breaks, is this allowed?**

   Occasional usage of university computer and network resource for non-work related activities are generally acceptable, as long as the activities do not interfere with performance of your job or other university responsibilities. Further, the non-work related activities must not include any prohibited actions as described in this policy including use of computer or network resources to access sexually explicit materials in violation of Va. Code 2.2-2827. Use of social media sites for work-related reasons must be conducted in accordance with this policy.

6. **If I am using my own computer or electronic device on the VCU wireless network, do I have to abide by these policies?**

   Yes. While the computer or electronic device may belong to an individual, the use of VCU wired or wireless network subjects the individual user to this policy. Further, if you use personally-owned computers or electronic devices to conduct VCU work, those records must also be made available to the university and are subject to the Virginia Freedom of Information Act.

7. **Do I have to abide by this policy if I am just posting or uploading some content to some other resource on the Internet from a VCU Computer or Network Resource?**

   Yes. This policy covers the use of VCU computer or network resource to generate, access, modify, view, download, post, upload, store, and / or remove information. Any of the aforementioned actions utilizing VCU Computer and Network Resources are regulated under this policy.

8. **I use my computer on the VCU network to save files and access resources on a third party website or another cloud based service, do I have to abide by this policy?**

   Yes. Regardless of the device used and service accessed, the use of VCU wired or wireless network subjects the individual user to this policy.