Information Technology
Student / General Patron Acceptable Use Agreement
Applicable to all Users of College Computing Resources

Version: 4.0
Status: Final 09/27/2024
Contact: Chief Information Security Officer, VCCS Information Technology Services

---

Agreement

I acknowledge that this college is part of the Virginia Community College System (VCCS), home to Virginia's 23 community colleges. As a user of the college's local and shared computer systems, I understand and agree to abide by the following acceptable use agreement terms. These terms govern my access to and use of the information technology applications, services and resources of the VCCS, the college, and the information they generate.

9.5 Acceptable Use of VCCS Information Technology (IT) Resources

9.5.0 Purpose

Appropriate organizational use of information and Information Technology ("IT") resources and effective security of those resources requires the participation and support of the VCCS college faculty, staff, students, and others "Users"). Inappropriate use exposes VCCS colleges to potential risks, including virus attacks, compromise of network systems and services, and legal issues. This agreement provides rules for the acceptable use of all information technology resources, including computers, applications, software, hardware, communication services, cloud-based services, and networks owned, managed, or operated by the Virginia Community College System (VCCS).

9.5.1 Scope

This agreement applies to any person using VCCS-owned and/or managed information technology resources to transmit, process, manage, and/or store electronic data. This includes all persons assigned user accounts managed by the VCCS for email communications and to enable Network and/or Application access, as well as all persons who may access such services that are owned and/or managed by the VCCS.

In addition, users must read and understand the VCCS Information Security Policy and associated policies and standards.

9.5.2 Definitions

Application - An automated solution (computer program) designed to fulfill one or more business functions. It may be a single program designed for a single business function or a multi-module/program or multi-sub-system entity with modules/programs/components that support multiple business functions.

Authorization - The process of granting access to data or information systems by the designated authority after proper identification and authentication.

Computer - A device that accepts information in digital (typically binary) or similar form and manipulates it for a result based on a sequence of instructions. This includes laptop computers, desktop computers, tablets, communication devices such as smartphones, and many internet-connected devices such as control processors.

Information Technology (IT) - The hardware and software owned, managed, or operated by an organization to support the flow or processing of information in support of business activities, regardless of the technology involved, whether computers, telecommunications, or others. In the Commonwealth of Virginia, Information Technology means telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services. Information Technology includes a Computer and computing resources. See also Computer.

Mobile Computing Device – A computer device designed to be portable, which may be connected to a network using wireless communication technologies, including but not limited to notebooks, palm devices, laptops, smart cards, and mobile phones.

Network- A configuration of data processing devices and software connected for information interchange allowing a group of two or more computers to be linked together to facilitate data transmission between devices.

Sensitive Data - Any data that, if compromised with respect to confidentiality, integrity, and/or availability, could have a material adverse effect on the Commonwealth's interests, the conduct of the VCCS or other agency programs, or the privacy to which individuals are entitled.

User – Any individual who utilizes VCCS information technology resources and services, including all employees (faculty, adjunct faculty, staff), contractors, students, and guests of the VCCS. Users may be assigned a user account to facilitate authentication of identity and authorization of access to and uses of network services and applications.

User Account – An electronic identity assigned to an individual to allow authorized access to information technology services, usually consisting of a username and password or another secret token used to authenticate the user.

9.5.3 Agreement Statement

Thousands of Users share Virginia Community College System(VCCS) Information Technology (IT) resources, facilitating the mission of the VCCS to provide teaching, instruction, and learning opportunities for the public. All Users are responsible for using these resources appropriately, respecting the rights of others. All uses of information and information technology resources must comply with organizational policies, standards, processes, procedures, and any applicable license agreements, contracts, and intellectual property laws, including federal, state, and local laws. Misuse of these resources by even a few individuals has the potential to disrupt business or the work of others. Persons violating this agreement may be subject to

disciplinary action. Violations of this agreement may also violate federal, state, or local laws.

9.5.4 Information Access

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the organization's IT resources or any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner, including in real-time, and used or disclosed in any manner by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of IT resources used, including but not limited to computer files and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems, and other electronic records).

VCCS colleges may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. For example, VCCS colleges may block access to certain websites or services that do not serve legitimate organizational or academic purposes or may restrict users' ability to attach devices to the college's IT resources.

9.5.5 Acceptable Use Requirements

a) All information and information technology resource uses must comply with organizational policies, standards, processes, procedures, and any applicable license agreements, contracts, and intellectual property laws, including federal, state, and local laws.

b) Users must use only those information technology resources they have been granted the authority to use, and users must use VCCS computer resources only for authorized purposes.

c) Users must not provide false or misleading information to gain access to computing resources. Users must not use VCCS IT resources to gain unauthorized access to information technology resources of other institutions or persons. The VCCS will regard these actions as violations of VCCS policy and as criminal acts and may treat them accordingly.

d) Users acknowledge that the monitoring of IT systems and data may include but is not limited to (a) network traffic; (b) Application and data access; (c) keystrokes when required to support authorized security investigations; (d) user commands; (e) email and Internet usage; and (f) message and data content.

e) A Logon banner authorized by the Chief Information Security Officer of the VCCS shall be used on all VCCS end-user devices to communicate that VCCS IT systems may only be used for authorized purposes, their use may be monitored at any time and that there is no expectation of privacy when using a VCCS IT resource.

f) Local Administrator rights or the equivalent of such on non-Microsoft Windows-based IT computer systems shall be limited only to authorized staff as appropriate to prevent users from intentional or accidental modification of the

operating system, installed applications, security controls, or the adding or removal of hardware components.

g) Users must report any violation of this agreement by another individual and any concerns related to cybersecurity to the Information Security Office or the Director of Internal Audit. Users must assist VCCS officials with investigating violations of this agreement.

h) The VCCS shall document the user's acceptance of this Acceptable Use Agreement before or as soon as practicable after gaining access to VCCS IT systems.

9.5.6 Prohibited Uses

a) Any use that is in violation of applicable local, state, and federal law.

b) Users must not authorize anyone to use their computer accounts for any reason and are responsible for all use of their accounts. Users must take all reasonable precautions, including password maintenance and file protection measures, to prevent unauthorized use of their accounts. Users must not, for example, share their password with anyone.

c) The transmission of unencrypted sensitive data over the Internet is prohibited. When connected to internal VCCS networks from non-VCCS networks, users shall use a VCCS-approved virtual private network (VPN) connection. When transmitting sensitive data over the Internet the data must be encrypted and sent using secure file transfer services and protocols.

d) Use of any external Network or Application services while connected to any VCCS IT resource must comply with this agreement.

e) Other than material known to be in the public domain, users must not access, alter, copy, move, or remove information, proprietary software, or other files (including programs, members of subroutine libraries, data, and electronic mail) without prior authorization.

f) Users must not distribute or disclose third-party proprietary software without prior authorization from the licenser. Users must not install proprietary software on systems not properly licensed for their use.

g) Users must not use any VCCS IT resources to access, upload, download, transmit, print, post, or store information with sexually explicit content as defined in and prohibited by law (see Code of Virginia § 2.2-2827).

h) Users must not use any VCCS computer, computer system, or computer network to harass, stalk, or threaten others or to otherwise violate state, local, or federal law or university policies Section 3 – Human Resources, General Policies, Section 3.14 and Section 6 - Student Development Services, Campus Conduct, Section 6.5.

i) Users must not intentionally, recklessly, or negligently damage computer systems, intentionally damage or violate the privacy of others, intentionally misuse VCCS IT resources, or allow the misuse of VCCS IT resources by others.

j) Users must not use the VCCS's Internet access or electronic communication in cases where it:

- interferes with the user's productivity or work performance or with any other employee's productivity or work performance,
- adversely affects the efficient operation of the computer system,
- results in any personal gain or profit to the user, or
- violates any provision of this agreement, any supplemental agreement adopted by the VCCS's Internet or electronic communication systems, or any other policy, law, or guideline as set forth by local, state, or federal law.

k) When using mobile computing and communication devices, users must ensure that work-related information is not compromised. Users should avoid using public Internet access for business purposes unless using an approved virtual private network connection.

9.5.7 Responsible Use

a) Users must not transmit restricted college, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo).

b) Users must not store restricted organizational, non-public, personal, private, sensitive, or confidential information on a non-organizational issued device, or with a third-party file storage service that has not been approved for such storage by the college. Devices that contain sensitive information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems when on travel.

c) Users are routinely assigned or given access to VCCS IT equipment in connection with their official duties or responsibilities. This equipment belongs to VCCS and must be immediately returned upon request or at the time a user is separated from the VCCS. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to VCCS. Should VCCS IT equipment be lost, stolen, or destroyed, users must provide a written report of the incident's circumstances. The VCCS has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

d) The use of public social media sites to market organizational activities requires pre-approval from the VCCS.

Institutional Accounts used to manage VCCS social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow information security standards, be unique on each site, and not be the same as passwords used to access other IT resources.

Users may not use their personal social media accounts for official business unless specifically authorized by VCCS. A disclaimer is strongly recommended if a personal email, posting, or other electronic message could be construed as an official communication. A disclaimer might be: “The views and opinions expressed are those of the author and do not necessarily reflect those of the VCCS.”

9.5.8 State Laws and Policies

a) All users of VCCS IT resources must adhere to *Virginia Department of Human Resource Management Policy 2.35 - Use of Internet and Electronic Communication Systems*.

b) All users of VCCS IT resources must adhere to *Virginia Department of Human Resource Management Policy 1.75 - Civility in the Workplace.*.

c) All users of VCCS IT resources must adhere to *The Virginia Computer Crimes Act, Article 7.1 of Title 18.2 of the Code of Virginia.*

9.5.9 Enforcement Procedure

a) The VCCS may temporarily revoke access to VCCS IT systems to limit damage to the systems and to investigate allegations of violations of this agreement.

b) Leadership will take disciplinary action following established policies and procedures.

c) The Chancellor or designee and college president or designee will report any violations of state and federal law to the appropriate authorities.

d) Colleges may adopt additional procedures consistent with this agreement.

Acknowledgement

I understand that it is my responsibility to read and abide by this agreement, even if I do not agree with all the terms and conditions indicated herein. If I have any questions about the VCCS Acceptable Use Agreement, it is my responsibility to contact the college Information Security Officer or appropriate college official for clarification.

By acknowledging this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that should I violate this agreement, I will be subject to disciplinary action.

Printed Name	Date	Signature