

Cape Cod Community College

Information Technology Resources Use Policy

General Principles

This document formalizes the policy for faculty, staff, students (both full and part-time) and all other individuals who have been granted use of the information technology resources of Cape Cod Community College (CCCC) ("Users"). This policy and CCCC's "Code of Conduct" govern access and use of the College's electronic information and information systems originating from non-CCCC computers, including personal computers and other electronic devices. The use of information systems acquired or created through use of College funds, including grant funds from contracts between the College and external funding sources (public and private), are covered by this policy. This includes College information systems that are leased or licensed for use by members of the CCCC community.

Information technology resources include, but are not limited to: computers, local and wide area networks, printers, other peripherals, software systems, data, electronic mail, and the Internet.

Access to CCCC's computer systems and networks imposes certain responsibilities and obligations as set forth in this document. Users are granted use of information technology resources subject to College policies, and local, state and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individual rights to privacy.

Use of CCCC's information technology resources shall constitute acceptance of the terms of this policy and any other applicable College policies, rules and procedures.

Remainder of Page Intentionally Left Blank

Specific Principles

<u>Definitions</u>	Internet-Based Video Conferencing
<u>User Responsibilities</u>	<u>Data Ownership and Confidentiality</u>
<u>No Expectation of Privacy</u>	<u>Copyright Protection</u>
<u>Acceptable Use</u>	<u>Malicious Code</u>
<u>Unacceptable Use</u>	<u>Network Security</u>
<u>Restricted Services</u>	<u>E-Mail</u>
<u>Social Media</u>	<u>Internet Use</u>
Professional Social Media	<u>College Facebook Page</u>
Cloud Services	<u>Data Confidentiality</u>
Data Sharing Tools	<u>BYOD</u>
Third Party Email Services	<u>Violations</u>
Email Auto-Forwarding	<u>No Warranties</u>
Texting	<u>Enforcement</u>

Definitions

Availability – The expectation that information is accessible by CCCC when needed.

Cloud Services – Consumer and business products, services and solutions delivered and consumed on-demand, using the cloud service providers’ pooled resources, and delivered over a broad network, such as the Internet.

Confidentiality – The expectation that only authorized individuals, processes, and systems will have access to CCCC’s information.

Confidential Information – The most sensitive information which requires the strongest safeguards to reduce the risk of unauthorized access or loss. Unauthorized disclosure

or access may (1) subject CCCC to legal risk, (2) adversely affect its reputation, (3) jeopardize its mission, and (4) present liabilities to individuals (for example, HIPAA and HITECH penalties).

HIPAA – Health Insurance Portability and Accountability Act of 1996.

HITECH – Health Information Technology for Economic and Clinical Health Act.

Information System – Consists of one or more components (e.g., application, database, network or web) that is hosted in a CCCC campus facility, and which may provide network services, storage services, decision support services, or transaction services to one or more business units.

Integrity – The expectation that CCCC’s information will be protected from improper, unauthorized, destructive or accidental charges.

Internal Information – Data that is owned by the College, is not classified Confidential or Private, and is not readily available to the public. For example, this includes employee and student identification numbers and licensed software.

Mobile Computing Device – Including, but not limited to, laptops, netbooks, tablets, smartphones (BlackBerry, iPhone, etc.) and mobile broadband cards (also known as AirCards® and connect cards).

Private Information – Sensitive information that is restricted to authorized personnel and requires safeguards, but which does not require the same level of safeguards as confidential information. Unauthorized disclosure or access may present legal and reputational risks to the College.

Privileged Information – Refers to attorney-client communication.

Public Information – Information that is readily available to the public, such as the information published on web sites.

Removable Media – Including, but not limited to, CDs, DVDs, copier hard drives, storage tapes, flash devices (e.g., CompactFlash and SD cards, USB flash drives), and portable hard drives.

Social Media – Refers to tools that allow the sharing of information and creation of communities through online networks of people.

CCCC Community – Faculty, staff, non-employees, students, contractors, covered entities, agents, and any other third parties of CCCC.

User Responsibilities

All information technology resources are owned and operated by Cape Cod Community College as an agency of the Commonwealth of Massachusetts. The College reserves all rights to these resources. It is the responsibility of any person using CCCC information technology resources to read, understand, and comply with this policy. Additionally, Users must comply with all other applicable College policies and procedures as well as state and federal laws. Any questions regarding this policy should be directed to the Vice President of Finance and Operations.

An account or user ID is issued to faculty, staff and students when they begin their employment or studies with the College. An account or user id permits access to information technology resources. This account or user ID is removed upon termination of one's employment with the College or completion or withdrawal from an academic program.

No Expectation of Privacy

CCCC information technology resources are the property of Cape Cod Community College and the Commonwealth of Massachusetts and are to be used in conformity with this policy. Information created, stored, or accessed using CCCC information systems may be accessed and reviewed by CCCC personnel to measure, monitor, and address the use, performance or health of the College's information systems, or to respond to information security issues. Internet usage may also be monitored when using the College's network, including when using CCCC's remote access services. Additionally, data backups of electronic information stored on CCCC's information systems are made regularly and stored at off-site locations or across the campus.

This information may be provided to an external party at the College's direction without prior notification. Therefore, users have no expectation of privacy when accessing, transmitting, receiving, creating, or storing personal information using the College's information systems (particularly, network services). This includes access to the Internet through a College information system, unless such communications are protected by law or privilege.

All electronic information created, stored or transmitted by use of CCCC's information systems is the property of the College, unless otherwise explicitly noted.

A. Requirements:

President/ CEOs, Vice Presidents and Deans must:

1. Distribute copies of this policy to all members of their organizations.
2. Ensure that each member of their respective organizations receives periodic training and awareness about acceptable use of the College's electronic information and information systems.
3. Communicate any additional restrictions they have established governing their members use of the College's electronic information and information systems.

When reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, CCCC will exercise the right to inspect any User's computer, any data contained in it, and any data sent or received by that computer. Use of CCCC information technology resources constitutes express consent for CCCC to monitor network activity in any form that CCCC sees fit to maintain the integrity of the network. Therefore, Users shall have no expectation of privacy over any communication, transmission or work performed using CCCC information technology resources.

Acceptable Use

The College's information technology resources and services may be used only for academic, educational, or professional purposes which are directly related to official College business and in support of the College's mission. They are not provided for personal use. The use of information technology resources is integral to enhancing productivity in the daily office routine and enabling faculty, staff, and students to make use of research and educational opportunities. The College expects users will access and use the College's electronic information and information systems in a manner that:

1. Does not compromise the confidentiality, integrity, or availability of those assets; and
2. Reflects the College's standards as defined in the Code of Conduct and its body of policies, and in accordance with all applicable federal, state, and local laws governing the use of computers and the Internet.

These obligations apply regardless of where access and use originate: CCCC office, classroom, public space, lab, at home, or elsewhere outside the College.

The rules stated in this policy also govern the use of information assets provided by the State of Massachusetts, other state and federal agencies, and other entities that have contracted with CCCC to provide services to their constituents and / or clients.

Schools, units, and departments may produce more restrictive policies. Therefore, users should consult with their department if there are any other restrictions in place that supplement this policy.

Acceptable information technology uses may include but are not limited to:

- ❖ Using classroom and lab computers for class assignments
- ❖ Preparing instructional materials
- ❖ Publishable research
- ❖ Personal computing to improve computer literacy and to learn new software and/or hardware
- ❖ Accessing generally available individual and campus information
- ❖ Using the technology to support faculty and staff in performing their work
- ❖ Authorized and approved use of the College's information and administrative systems
- ❖ Using the Internet to promote collegial and professional interaction, research and productivity

In making acceptable use of resources you must:

- ❖ Use resources only for College business, for purposes authorized by the College.
- ❖ Use the College web site, server and all other related computer equipment and services only for academic, educational or professional purposes which are directly related to official College business and in support of the College's mission.
- ❖ Be responsible for all activities conducted on your user ID or that originate from your system that result from your negligent failure to protect your user ID or to protect against such unauthorized use.
- ❖ A user is prohibited from disclosing his / her user ID to anyone for use on the College's computer network.
- ❖ Access only files and data that are your own, that are publicly available, or to which you have authorized access.
- ❖ Use only legal versions of copyrighted software in compliance with vendor license requirements.
- ❖ Be considerate in your use of shared resources. Examples include not monopolizing systems, overloading networks with excessive data, or wasting computer time or resources, disk space, printer paper, manuals or other resources.

Unacceptable Use

The list of prohibited actions is not intended to be comprehensive. The evolution of technology precludes the College from anticipating all potential means of capturing and transmitting information. Therefore, users must take care when handling sensitive information.

In making acceptable use of resources you must NOT:

- ❖ Distribute information classified as Confidential or Private, or otherwise considered or treated as privileged or sensitive information, unless they are an authoritative College source for, and an authorized College distributor of, that information and the recipient is authorized to receive that information.
- ❖ Share their passwords with other individuals or institutions (regardless if they are affiliated with the college or not) or otherwise leave them unprotected.
- ❖ Use another person's user ID or password.
- ❖ Use another person's files or data without permission.
- ❖ Use third party email services to conduct sensitive College business or to send or receive College information classified as Confidential or Private, or otherwise considered privileged or sensitive information.
- ❖ Use computer programs to decode passwords or access control information.
- ❖ View, download, store or transmit child pornographic materials or obscene materials. Materials are considered obscene if: (1) the average person, applying community standards, would find the material appeals to the prurient interest; (2) the materials describes or depicts sexual conduct in a patently offensive manner; and (3) taken as a whole, the material lacks serious literary, artistic, political or scientific value.
- ❖ Circumvent, subvert, or attempt to circumvent or subvert system or network security measures.
- ❖ Purposely engage in any activity that might be harmful to system / network or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- ❖ Pursuant to Massachusetts Campaign Finance Laws, no governmental resources (including computers, fax machines, modem, printers, and / or copy machines) may be used by any person (including a public employee, whether during work hours or otherwise) in order to promote or oppose a political candidate. Further, in addition to a prohibition of any type of political fundraising on State property, a public employee is further prohibited from soliciting or receiving, directly or indirectly, any contribution for political purpose.
- ❖ Make or use illegal copies of copyrighted software, store such copies on College systems, or transmit them over College networks.
- ❖ Use the network for purposes which place a heavy load on scarce resources.
- ❖ Use Cape Cod Community College's computers or networks to libel slander or harass any other person. The following shall constitute Computer Harassment: (1) using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such

communication to cease (such as debt collection); (3) using the computer to disrupt or damage the academic research, administrative, or related pursuits of another; (4) using the computer to invade the privacy, academic or otherwise, of another or threatened invasion of privacy of another.

- ❖ Waste computer resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- ❖ Use the College's systems or networks for personal gain; for example, by selling access to your user ID or to College systems or networks, or by performing work for profit with College resources in a manner not authorized by the College.
- ❖ Use the College's or any other College-related systems or networks to transmit any material in violation of United States or Massachusetts laws or regulations.
- ❖ Engage in recreational game playing or online gambling.
- ❖ Intercept communications intended for other persons.
- ❖ Misrepresent either the College or a person's role at the College.
- ❖ Infringe on any intellectual property rights.
- ❖ Distribute chain letters.
- ❖ Engage in any other activity that does not comply with the General Principles presented above.

This list of unacceptable uses is not intended to be exhaustive.

Restricted Services

This list of restricted services is not intended to be comprehensive. The evolution of technology precludes the College from anticipating all potential means of storing, capturing and transmitting information. Therefore, when using third party technology services not explicitly restricted in this policy, users must exercise care to not compromise the sensitive CCCC information.

Restricted services include the following:

1. **Social Media** - The use of all College computer resources for social media activities including, but not limited to, Facebook, YouTube, Twitter, blogs or other form of social media, shall comply with this policy. Use of the College's computer resources by faculty and staff for personal social media activities is prohibited. Use of the College's computer resources by students for educational and social activities consistent with the College's mission shall comply with this policy.
 - A. Social media tools cannot be used to communicate or store College information classified as Confidential or Private or otherwise considered

privileged or sensitive by CCCC. Social media tools include, but are not limited to:

- Social networking sites: e.g. Facebook, Google+, Myspace, LinkedIn
- Blogs
- Micro blogging sites: e.g. Twitter
- Wikis
- Content-sharing services: e.g. YouTube (video) and Flickr (for photos, videos, etc.)

B. Online forums.

C. The Cape Cod Community College name or your CCCC email address cannot be used on social media sites for personal communications or postings.

D. Using the CCCC name or email address on social media sites to post information in a manner that may be interpreted as representing an official position of CCCC, or which may misrepresent the College's viewpoint. All posting where the user is identified as a member of CCCC should clearly communicate that, "The views and opinions expressed are strictly those of the author. The contents have not been reviewed or approved by Cape Cod Community College."

2. **Cloud Services**

A. Cloud Storage Tools - The use of third party cloud storage services cannot be used to store CCCC information classified as Confidential or Private or otherwise considered privileged or sensitive by CCCC. Cloud storage tools include, but are not limited to:

- iCloud
- OneDrive
- Office 365

B. Data Sharing Tools - The use of data sharing tools cannot be used to share or store CCCC information classified as Confidential or Private or otherwise considered privileged or sensitive by CCCC. Data sharing tools include, but are not limited to:

- Microsoft OneDrive
- Box.net

- Catch
- Dropbox
- Evernote
- Google Docs
- Google Drive

3. **Third Party Email Services** - Third party email services cannot be used to communicate or store CCCC information classified as Confidential or Private or otherwise considered privileged or sensitive by CCCC.
4. **Texting** - Users should take care texting other sensitive information, particularly when confirmation of receipt or the identity of the recipient is required for business or legal purposes.
5. **Internet-Based Video Conferencing** - Faculty and Staff - Internet-based video conferencing services, such as Skype, are limited to CCCC business-use only and must be conducting using CCCC equipment. They are to be used strictly for business collaboration between members of the College community or outside entities, or for educational purposes. Users must ensure that video communications are done in a setting that limits or restricts the possibility that non-authorized individuals from viewing or listening to sensitive information.

Please see policy notes below for additional information.

Data Ownership and Confidentiality

Data and information stored in the College's computers and associated systems belong to the College, and its dissemination and use must comply with the College's policies and procedures.

Users shall not access, release, use or disseminate confidential or proprietary information unless User is authorized by CCCC to do so and such access, release, use or dissemination is consistent with state and federal law.

Copyright Protection

Pursuant to the Digital Millennium Copyright Act, 17 U.S.C. Section 1203(i)(1)(A), any user of CCCC's technology resources who engages in copyright infringement shall have his / her access privileges terminated.

Computer software is intellectual property. Software publishers and vendors can be very aggressive in protecting their property rights from infringement. These

intellectual property rights extend to information published on the Internet, such as text and graphics.

Users who buy their own software agree to comply with any and all provisions of the software vendor in the software license agreement. Users are not permitted to copy software made available by the College to any other computer. In instances where a license agreement links a license number to specific computers by serial number, and the hardware is replaced or upgraded, the license agreement but be changed accordingly.

In instances where the College holds a site license, Information Technology Services (ITS) holds the site license. Even though copying for College use is allowed for these types of agreements, it must be done in coordination with ITS.

All software on all computers on campus must be properly licensed. ITS maintains inventories of all computers and all software products installed on each computer. When users have made their own software purchases, it is their responsibility to furnish a license agreement when audited.

Malicious Code

Viruses, worms, Trojan horses, and other malicious code can be embedded in text files, executable files, graphics, word processing documents, spreadsheets and e-mail messages. The College uses technical methods, such as anti-virus, anti-spyware, and anti-SPAM software, to reduce the probability of a successful attack or infection. Users should exercise reasonable precautions in order to prevent the introduction of malicious code. Users should exercise reasonable precautions in order to prevent the introduction of harmful files. Users should not disable virus scanning utilities and such use such utilities to scan files downloaded from the Internet or obtained from a questionable source, and to scan portable media such as floppy disks, compact disks, and universal serial bus (USB) sticks.

Network Security

CCCC computers are connected to a local area network, which links computers through the College and through the wide area network to computers in other locations. All users should avoid compromising the security of the network. Users should **never** share their passwords with anyone else and should promptly notify ITS personnel if they suspect their passwords have been compromised. Users who leave their computers unattended for extended periods should either log off the network or have password-protected screen savers enabled.

E-Mail

Microsoft Office 365 is the official College e-mail system.

Electronic mail is a tool provided by the College to complement traditional methods of communications and to improve administrative and education efficiency. All e-mail accounts and all data transmitted or stored using e-mail facilities are owned by the College.

Broadcast messages to all staff and faculty using the #CCCC Faculty/Staff e-mail group should be used only for essential College announcements of concern to the entire College community.

All users should consider e-mail messages to be the equivalent of formal written communications and thus, should be professional and courteous in tone. Remember that an e-mail message can be stored, copied, printed, or forwarded to recipients. A general rule of thumb is not to put anything in an e-mail message that you would not write in a memorandum, nor be willing to post on a bulletin board or discuss in a public meeting.

Public Folders within Outlook are provided as a service for posting general news, events, and other College-related information. These folders will be monitored by those responsible for their content. Any posted material deemed inappropriate will be removed without prior notification. Public Folders are also subject to specific guidelines suitable for that particular folder.

Internet Use

The Internet is a useful tool for supporting many types of academic and business-related research. The College is committed to promoting responsible Internet access. All users should view Internet access as a privilege.

Users should be aware that many web sites gather and store information about visitors to their site. Care should be taken when registering for anything online, since this is analogous to giving your name, address and phone number to a stranger.

Users must be aware of the potential for malicious code to be introduced onto the College network and computers by downloading and installing files from websites, even those that seem innocuous. Users should be extremely cautious when making decisions about downloading software from the Internet.

Users must be aware of the College's limited Internet bandwidth. In addition to adhering to the College's policy regarding acceptable and unacceptable uses, Users are

discouraged from activities that consume large bandwidth, particularly during the peak daytime use periods. A single user can have a serious detrimental impact on all College users by failing to follow this recommendation.

College Facebook Page

The College encourages interaction from Facebook users but is not responsible for comments or wall postings made by visitors to the page. Comments posted also do not in any way reflect the opinions or policies of the College. The College is not responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the posting of any information on this page. The College reserves the right, but assumes no obligation, to edit or remove any posts and to block or remove members from the group. Posts promoting commercial or political activities or other non-College related ventures are prohibited. The College reserves the right to remove any content from the College's Facebook Page that is not consistent with this policy or any other College policies.

Data Confidentiality

In the course of performing their jobs, College employees often have access to confidential or proprietary information, such as personal data about identifiable individuals, student record information or commercial information about business organizations. Under no circumstances may employees acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs. These restrictions are in addition to restrictions or prohibitions over the release of confidential information contained under state or federal law.

Under no circumstances may employees utilize any of the College's or College-related systems or networks to store or transmit any confidential information that they have rightful access to unless required by their jobs. These restrictions are in addition to restrictions or prohibitions over the release of confidential information under state or federal law.

BYOD

TO BE ADDED

Violations

Failure to observe this policy may subject individuals to disciplinary action, including, but not limited to, loss of access rights, expulsion, termination of employment, and / or referrals to appropriate authorities in the event of violations of state or federal laws.

No Warranties

CCCC makes no warranties of any kind, whether express or implied, for the service it is providing. CCCC will not be responsible for any damages a User suffers. This includes loss of data resulting from delays, no-deliveries, or service interruptions caused by CCCC negligence or by the User's errors or omissions. Use of any information obtained via the Internet is at the User's own risk. CCCC specifically denies any responsibility for the accuracy or quality of information obtained through its services. Users need to consider the source of any information they obtain and consider how valid that information may be. Additionally, CCCC is not responsible for lost or deleted documents, files, e-mails, and other electronic resources.

CCCC also specifically denies any responsibility for a User's encounter, access or use of any inappropriate or controversial materials from CCCC information technology resources, including the Internet. Users must notify the Executive Director of Information Technology if they identify information technology resources being used in a manner inconsistent with these policies.

Enforcement

College officials will review alleged violations of acceptable use policies on a case-by-case basis. Violations of policy will result in appropriate actions, consideration of appropriate disciplinary measures and/or referral to appropriate authorities responsible for enforcing state and federal laws. Users who breach this policy may be denied access to the College's computer and communications networks and may be subject to further disciplinary action. When discipline is imposed, it shall be consistent with the terms of any governing collective bargaining agreement as applicable. In order to prevent further possible unauthorized activity, the College reserves the right to disconnect that user from the network. If this is deemed necessary by College staff, where appropriate, reasonable effort will be made to inform the user prior to the disconnection. Breaches of this Computer and Network Usage Policy will be referred to appropriate administrators for consideration of discipline in accordance with applicable College policies and procedures. The College considers any violation of acceptable use of principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on College systems allegedly relating to unacceptable use. Violators are subject to disciplinary action as prescribed in student and employee policies, handbooks, or contracts. Offenders also may be prosecuted under laws including (but not limited to) the Privacy Protection Act of 1974, The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989,

Interstate Transportation of Stolen Property, Family Educational Rights and Privacy Act (20 U.S.C. Section 1223g), Massachusetts Wiretap Statute (G.L. c.272, Section 99), Massachusetts Privacy Statute (G.L. c 214, Section 1B), Copyright Infringement laws (17 U.S.C. Section 101 et seq.), the Communications Decency Act of 1996 [47 U.S.C. Section 223 (d) - (h)], and the Electronic Communications Privacy Act of 1986 (18 U.S.C. Sections 2510-21, 2701-10, 3121-27). Access to the text of these laws is available through the Reference Department of the Library of Cape Cod Community College.