

THE COLONIAL WILLIAMSBURG FOUNDATION INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

Version 2

Abstract

The Colonial Williamsburg Foundation has established this policy concerning the acceptable use of critical technology resources and services by its employees, contractors, volunteers, and interns.

Kimberly M. Peay

Information Security Manager/ ISO




Table of Contents

Abstract	1
Overview	3
Purpose	3
Scope	3
Administration of this Policy	4
<i>Policy</i>	4
Security and Access	4
No Expectation of Privacy	4
Network Systems	5
Downloading and Installing Software/Website Agreements	5
Confidentiality and Proprietary Rights	6
E-mail and Text Messaging	6
Spam	6
Etiquette	7
Personal Use of Colonial Williamsburg-provided E-mail	7
Phishing	7
Internet	7
Personal Use of the Internet	8
Social Media	8
Computers and Laptops	8
Removable Storage Media	9
Mobile Devices	9
Lost or Stolen Devices or Data	9
Telephone and Voicemail	10
Personal Use	10
Inappropriate Use of Colonial Williamsburg IT Resources and Communications Systems	10
Corrective Action	10
Conduct Not Prohibited by This Policy	10
Additional Resources	11

Overview

This Policy covers use of and access to the Colonial Williamsburg Foundation's computers, networks, communication systems and other information technology resources. The IT resources and communications systems are intended for business purposes only (except for the limited personal use described below) during working time and at all other times. To protect CWF and the Colonial Williamsburg Company ("CWC" and collectively with CWF, "Colonial Williamsburg"), and their respective employees, contractors, volunteers and interns, it is CWF's policy to restrict the use of the IT resources and communications systems as described below. Each user is responsible for using the IT resources and communications systems in a productive, ethical and lawful manner.

CWF's and CWC's policies prohibiting harassment apply to the use of the IT resources and communications systems. No one may use a communications or computer system in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state or local law.

Purpose

The purpose of this Policy is to protect you and Colonial Williamsburg. Inappropriate use exposes Colonial Williamsburg to risks, including, but not limited to, virus attacks, compromise of network systems and services, loss or exposure of data, and legal issues.

Scope

This Policy applies to all users of Colonial Williamsburg's IT resources and communications systems, including employees, contractors, volunteers, and interns of Colonial Williamsburg. The use of the IT resources and communications systems by an employee, contractor, volunteer or intern of CWF and/or CWC shall signify his or her understanding of an agreement to the terms and conditions of this Policy, as a condition of employment or engagement, as applicable. As used in this policy, "you" means the employee, contractor, volunteer or intern of CWF and/or CWC, as applicable.

This Policy applies to all IT resources and communications systems owned or leased by Colonial Williamsburg, or otherwise made available at CWF and/or CWC, and all use of such resources and systems when accessed using your own resources, including but not limited to:

- Email systems and accounts
- Internet and intranet access
- Telephones and voicemail systems, including wired and wireless phones, smartphones and devices
- Printers, photocopiers, and scanners
- Fax machines, e-fax systems, and modems
- All other associated computer, network and communications systems, hardware, peripherals, and software, including network key fobs and other devices
- Closed-circuit television and other physical security systems and devices, including key cards and fobs

Administration of this Policy

The Information Technology Department (IT Department) is responsible for the administration of this Policy. If you have any questions regarding this Policy, please contact the IT Department.

Policy

The IT resources and communications systems are the property of CWF and are to be used for legitimate business purposes. CWF permits CWC and its employees, contractors, volunteers, and interns to access and use the IT resources and communications systems of CWF. You are provided access to the IT resources and communication systems to assist you in the performance of your job. You have the responsibility to use the IT resources and communications systems in a professional, lawful and ethical manner.

Security and Access

Security of the Information Technology (“IT”) resources and communication systems is the responsibility of the IT Department, including approval and control of your and others’ access to systems and suspension or termination of access in cases of misuse and you are no longer an employee, contractor, volunteer, intern or other authorized user, or otherwise ineligible to use the systems.

It is your responsibility to adhere to the IT security guidelines, including, but not limited to the creation, format and scheduled changes of passwords. All usernames, passcodes, passwords, and information used or stored on CWF’s computers, networks and systems are the property of CWF and/or CWC, as applicable. You may not use a username, passcode, password or method of encryption that has not been issued to you authorized in advance by CWF.

You may not share usernames, passcodes or passwords with any other person. You must immediately inform the IT Department if you know or suspect that any username, passcode or password has been improperly shared or used, or that IT security has been violated in any way.

No Expectation of Privacy

All contents of the IT resources and communications systems are the property of CWF and/or CWC, as applicable. Therefore, you should have no expectation of privacy whatsoever in any message, file, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind or form of information or communication transmitted to, received or printed from, or stored or recorded on the IT resources and communications systems.

You are expressly advised that in order to prevent against misuse, Colonial Williamsburg reserves the right to monitor, intercept and review, without further notice, every employee’s, contractor’s, volunteer’s and intern’s activities using the IT resources and communications systems, including, but not limited to, email (both incoming and outgoing), telephone conversations and voice mail recordings, instant messages and internet and social media postings and activities, and you consent to such monitoring by your acknowledgement of this Policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logs, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

CWF may also store copies of such data and communications for a period of time after they are created and may delete such copies from time to time without notice.

Do not use the IT resources and communications systems for any matter that you desire to be kept private or confidential from CWF and/or CWC.

CWC uses the IT resources and communications systems owned, leased and otherwise made available by CWF to CWC. CWF may disclose to CWC any and all contents of the IT resources and communications systems, including, without limitation, messages, files, data, documents, facsimiles, telephone conversations, social media posts, conversations or messages, or any other kind or form of information or communication transmitted to, received or printed from, or stored or recorded on the electronic information and communications systems, as they are sent to, received from, or otherwise relate to any CWC employee, contractor, volunteer or intern, or CWC's business.

Network Systems

Colonial Williamsburg maintains integrated computer and data communications networks to facilitate all aspects of its business. You may never sign on to any network equipment using the password or user name of another employee, contractor, volunteer or intern. You should not access, attempt to access, alter, or delete any network document except in furtherance of authorized Colonial Williamsburg business.

All work product related to Colonial Williamsburg must be stored on the Colonial Williamsburg network. Storing work product on personal computers, other locations and cloud storage, including, but not limited to, Dropbox, Google Drive, iCloud, etc. is prohibited without the express prior approval of the IT Department.

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and you must not perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, spending excessive amounts of time on the Internet, or otherwise creating unnecessary loads on network traffic associated with the non-business-related use of the Internet.

You are not permitted to "plug" any personally owned devices into Colonial Williamsburg's wired network. All systems and devices used to connect to Colonial Williamsburg's networks through remote access solutions must be virus free, must be continually executing virus scanning software with a current virus database, must have a firewall activated, and must use the most current version of operating system, with all security patches installed.

Downloading and Installing Software/Website Agreements

E-mail and downloading from the Internet are prime sources of viruses and other malicious software. Therefore, you may not download or install any software or shareware to your hard drive that is not expressly authorized or approved by the IT Department. In addition, employees may not accept the terms or conditions of website agreements without first obtaining approval from the IT Department.

Confidentiality and Proprietary Rights

Colonial Williamsburg's confidential information and intellectual property (including trade secrets) are extremely valuable to Colonial Williamsburg. Treat them accordingly and do not jeopardize them through your business or personal use of electronic communications systems, including e-mail, text messaging, internet access, social media and telephone conversations and voice mail. Ask your manager if you are unsure whether to disclose confidential information to particular individuals or how to safeguard the company's proprietary rights.

Do not use Colonial Williamsburg's name, brand names, logos, taglines, slogans or other trademarks without written permission from Colonial Williamsburg's Legal Department.

This Policy also prohibits the use of the IT resources and communications systems in any manner that would infringe or violate the proprietary rights of third parties. Electronic communications systems provide easy access to vast amounts of information, including material that is protected by copyright, trademark, patent, and/or trade secret law. You should not knowingly use or distribute any such material downloaded from the internet or received by e-mail without the prior written permission of the CWF's Legal Department.

E-mail and Text Messaging

Colonial Williamsburg provides certain employees, contractors, volunteers and interns with access to e-mail and/or text messaging systems for use in connection with the performance of their job duties. Colonial Williamsburg seeks to provide stable and secure e-mail and text messaging systems (including SMS and internet-based instant messaging) with rapid, consistent delivery times that promote communication for business purposes without incurring unnecessary costs or generating messages that are unproductive for the recipient. Many of the policies described below governing use of the company's e-mail and text messaging systems are aimed at reducing the overall volume of messages flowing through and stored on the network, reducing the size of individual messages, and making the system more efficient and secure.

Spam

Unfortunately, users of e-mail will occasionally receive unsolicited commercial or bulk e-mail (spam) which, aside from being a nuisance and a drain on IT resources, might be a means to spread computer viruses and other malicious software. Avoid opening unsolicited messages and report any suspicious e-mail to the administrator. Delete all spam immediately. Do not reply to the message in any way, even if it states that you can request to be removed from its distribution list. If delivery persists, contact the IT Department who will block any incoming e-mail from that address. Email should only be used for Colonial Williamsburg business. You are not permitted to use the email system for distributing spam or for pyramid or chain letters or other junk email.

Etiquette

Proper business etiquette should be maintained when communicating via e-mail and text messaging. When writing a business e-mail, be as clear and concise as possible. Sarcasm, poor language, inappropriate comments, attempts at humor, and so on, should be avoided. When communicating via e-mail or instant messages, there are no facial expressions and voice tones to assist in determining the meaning or intent behind a certain comment. This leaves too much room for misinterpretation. E-mail communications should resemble typical professional and respectful business correspondence.

Personal Use of Colonial Williamsburg-provided E-mail

Personal use of company-provided e-mail is permitted on non-working time only so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

Phishing

You should be wary of phishing – attempts to trick you into providing personal or financial information via an email request or through a link to a fraudulent website. Phishing is a criminal activity using various techniques to manipulate you into performing actions or divulging confidential information that you would not normally provide.

Phishing emails may appear to be from a trustworthy source but are designed to trick the email recipient into disclosing sensitive, private and confidential information. By clicking on an active link in a phishing email, the recipient may be directed to a fraudulent website that attempts to acquire personal or private information or possibly infect the computer with malicious software. To check the destination of an active link, you should hover your mouse over it and review the address information displayed in the status bar located at the bottom of the screen.

Emails that contain obvious spelling errors may be a phishing attempt. Phishers do this intentionally in order to avoid spam filters that many Internet providers use.

The email may contain links to the website contain all or part of a real entity's name or web address, but the link itself is not identical to that of the legitimate website. Clicking on these links may take you to a different, possibly malicious website or pop-up window that asks you to provide, update or confirm sensitive personal information.

If you have questions about whether an email you receive may be a phishing attempt, you should immediately contact the IT Department.

Internet

Colonial Williamsburg provides desktop Internet access to certain employees, contractors, volunteers, and interns for use in connection with the performance of their job duties. The following outlines Colonial Williamsburg's expectations regarding internet and social media access and use by employees.

Personal Use of the Internet

We recognize that you may occasionally desire to access the internet (including social media) for personal activities at the office or by means of the CWF's computers, networks and other IT resources and communications systems. We authorize such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity.

Using the Internet (including social media) to access pornographic, sexually explicit or "hate" sites, or any other website that might violate the law or Colonial Williamsburg's policies against harassment and discrimination is never permitted.

Personal use of the internet (including social media) is never permitted on working time or by means of the company's computers, networks and other IT resources and communications systems.

Social Media

Social media is technology that enables online users to interact and share information (including video, audio, photographs, and text) publicly or privately. Employees must adhere to Colonial Williamsburg's Social Media Policy & Principles.

Computers and Laptops

Colonial Williamsburg has a managed desktop policy to help protect the IT resources and communications systems from the threat of virus, malware, etc. A managed desktop policy restricts your right to install software and reduces the risk of being infected with malicious code. Only Colonial Williamsburg issued equipment is allowed to be connected directly to the Colonial Williamsburg network.

Colonial Williamsburg uses several levels of virus and spam monitoring. Upon any indication or notification of any infection, quarantine, or compromised by a virus, Trojan or malicious code, you must immediately stop using your computer and are required to contact the IT Department immediately. The IT Department may, at its discretion, remove and replace the computer.

Colonial Williamsburg may require other security measures to be taken to protect computers, such as logging out when your computer is not in use or inactivity timeouts. To prevent unauthorized access to the IT resources and communications systems and to ensure that security updates can be applied to Colonial Williamsburg's computers.

You must exercise caution when opening files, attachments or emails from unknown sources. If you are unsure of the validity of a file, attachment or email, please contact the IT Department.

You will be required to use passphrases as an alternative to passwords. What's the difference? A password typically consists of an eight-character entry, usually based on a set of random characters or even a single dictionary word with additional special characters and numbers. Passwords are now trivial to crack with today's modern technology.

The rule for how you will enter the "password" fields now requires longer entries when accessing CWF's networks. Changing the parameters of this one factor alone raises the length of time to an infeasible amount of time and resources to crack. Therefore, CWF will require the use of passphrases.

Passphrases can be a combination of words, letters, numbers, and special characters that can be easily remembered versus a long password.

The following password guidelines should be used to create strong easy to remember passphrases. They:

- Shall be a minimum of 14 characters in length.
- Shall be changed every 180 days
- Shall not reuse the last 24 passwords
- Should not be easily guessed information, such as personal information, names, pets, birth dates, etc.
- After 5 attempts, the user will have to wait 30 minutes to retry.

Removable Storage Media

Removable storage media, such as CD, DVD, flash drives (also known as jump/thumb/USB drives) or any other external storage devices should be used for business purposes only. Due to the amount of data this type of media will hold, these devices present a security risk and should be avoided when possible.

You must use extreme caution to keep this type of media secure to maintain confidentiality. Storage devices or removable media that contain Colonial Williamsburg data, information, files, emails, messages, or other content must be adequately erased prior to disposal or reuse. You should contact the IT Department for assistance.

Mobile Devices

Colonial Williamsburg supports specific protocols and devices, such as smartphones, tablets, and other approved devices, for the purpose of providing approved users with Colonial Williamsburg's email, calendar, and contacts. The IT Department will assist you, if you are an approved user, with the initial setup and will troubleshoot issues with Colonial Williamsburg data only. Passwords, encryption, inactivity timeouts or other security measures, such as virus protection, may also be required by Colonial Williamsburg. All other device operation and usage is your sole responsibility.

Colonial Williamsburg data, information, files, emails, messages and other content must be wiped by the IT Department before a mobile device is upgraded, recycled or discarded. In addition, Colonial Williamsburg data, information, files, emails, messages, and other content must be wiped by the IT Department upon your termination or separation.

Lost or Stolen Devices or Data

You are required to immediately report the loss of any storage device, including laptops, smartphones, tablets, notebooks, and removable storage media containing Colonial Williamsburg data to the IT Department. Colonial Williamsburg may be able to erase the device remotely. If so, Colonial Williamsburg is not responsible for the loss of any personal information or applications that may be contained on the device.

Telephone and Voicemail

Colonial Williamsburg provides landline and/or mobile telephone access and voicemail systems to certain employees for use in connection with the performance of their job duties. To ensure that our customers are provided with courteous and respectful service, and to prevent misuse of the IT resources, your telephone conversations and voicemail messages may, without notice, be monitored, recorded and reviewed. Colonial Williamsburg may also store recorded telephone conversations and voicemail messages for a period of time after they take place and may delete such recordings from time to time.

Personal Use

We recognize that employees might occasionally need to use company telephones and voicemail for personal activities. We authorize the occasional personal use of the company's telephones and voicemail systems so long as it does not comprise unprofessional or inappropriate conversations or messages and does not interfere with your employment responsibilities or productivity. Colonial Williamsburg telephones may not be used for commercial, religious or political solicitation, or to promote outside organizations.

Inappropriate Use of Colonial Williamsburg IT Resources and Communications Systems

You are never permitted to use Colonial Williamsburg's IT resources and communications systems, including e-mail, text messaging, internet access, social media, telephones, and voicemail, for any inappropriate or unlawful purpose. This includes but is not limited to:

- Misrepresenting yourself as another individual or company.
- Sending, posting, recording or encouraging receipt of messages or information that may be offensive because of their sexual, racist, or religious content.
- Revealing proprietary or confidential information, including official CWF and/or CWC information, employee information or intellectual property without authorization.
- Conducting or soliciting illegal activities.
- Representing your personal opinion as that of CWF and/or CWC.
- Interfering with the performance of your job or the jobs of other CWF and/or CWC employees, contractors, vendors or interns.

For any other purpose that violates Colonial Williamsburg's policies or practices.

Corrective Action

Employees, contractors, volunteer, and interns who violate any provision of this Policy are subject to discipline, up to and including termination.

Conduct Not Prohibited by This Policy

This policy is not intended to restrict communications or actions protected or required by state or federal law.

Additional Resources

For further information regarding Colonial Williamsburg's technology policy, process, and procedure, please refer to the Information Security Policy Manual and the Employee Handbook.

For technical assistance regarding such issues with email addresses contact the IT Department.

For assistance with employee management and supervisory issues, including investigations and corrective action, contact your supervisor or your Human Resources Generalist.

For assistance with retention and disposition of email, Internet content or related ancillary technologies' files, contact the Archives and Records Department.