UNION COUNTY PUBLIC SCHOOLS
TECHNOLOGY SERVICES

Acceptable Use Guidelines

Overview

Though there are a number of reasons to provide a user network access, the most important reason by far is so that the end user can complete the task(s) they wish to accomplish. Network access carries certain responsibilities and obligations as to what constitutes acceptable use of the UCPS network. The Internet is a resource that contains instructional value, and when used properly, can offer the end user infinite educational resources. These guidelines explain how UCPS information technology resources are to be used and specify what actions are prohibited. While these Acceptable Use Guidelines (AUG) are thorough, no set of guidelines can cover every situation, and thus the user is asked to additionally use sensible judgment when using UCPS technology resources. Questions on what constitutes acceptable use should be directed to the Chief Technology Officer (CTO) and/or Executive Team associated with these guidelines.

Purpose

The purpose of these guidelines is to detail the acceptable use of UCPS information technology resources for the protection of all parties involved.

Scope

These guidelines apply to any and all use of UCPS IT resources including, but not limited to, computer systems, personal mobile devices, email, network, and the UCPS Internet connection; however these guidelines do not supersede any Union County Board of Education policies.

E-mail Use

Personal usage of UCPS email systems is permitted as long as A) such usage does not negatively impact the UCPS computer network, and B) such usage does not negatively impact (bully, harass, etc.) parties involved.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.

- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to UCPS may not be sent via email, regardless of the recipient, without proper encryption.
- It is UCPS protocol not to open email attachments from unknown senders or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. Cloud storage environments such as Microsoft One Drive or Google should be utilized for sharing large data files.
- Language in emails should be appropriate and not contain profanity.

Confidentiality

Confidential data must not be A) shared or disclosed in any manner (this includes a student's username and password), B) posted on the Internet or any publicly accessible systems, or C) transferred in any insecure manner. It is dangerous to disseminate personal information (full name, address, DOB etc.) in an online setting.

Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not applicable to them. Existence of access capabilities does not imply permission to use this access. Additionally, UCPS is not responsible for data loss on UCPS devices. Access to UCPS or district cloud resources will be restricted upon graduation.

Unacceptable Use

The following actions shall constitute unacceptable use of the UCPS network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the UCPS network and/or systems to:

- Engage in activity that is illegal under local, state, federal, international, or other applicable laws.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to UCPS.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the learning environment.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of the employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Engage in activity that could harm the network and/or computer devices (virus).
- Stream music or play executable computer games.

Web Browsing

The Internet is a network of interconnected computers of which the district has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. Although a filter is in place, it is impossible to block every site that may be deemed offensive. The user must use the Internet at his or her own risk. UCPS is specifically not responsible for any information that the user views, reads, or downloads from the Internet. Additionally, UCPS is not responsible for the accuracy and/or quality of information obtained from the Internet. UCPS recognizes that the Internet can be a tool that is useful for both personal and professional purposes.

Copyright Infringement

UCPS computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the acceptable use guidelines, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs and DVDs, B) posting or plagiarizing copyrighted material, and C) downloading copyrighted files which the user has not already legally procured. This list is not exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above.

Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the UCPS network under any circumstance.

Streaming Media

Streaming media can use a great deal of network resources and may be limited or restricted.

Expectation of Privacy

Users should expect no privacy when using the UCPS network. Such use may include but is not limited to, transmission and storage of files, data, and messages. UCPS reserves the right to monitor any and all use of the computer network. To ensure compliance with district policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

Bandwidth Usage

Excessive use of UCPS bandwidth or other computer resources is not permitted.

Circumvention of Security

Using UCPS-owned computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited. If an individual is aware of someone circumventing security and/or demonstrating this to others, the individual should immediately alert Technology Services.

Software Installation

Numerous security threats can masquerade as innocuous software - malware, spyware, and trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. Therefore, UCPS approved software will be installed on applicable computers determined by the System Administrator.

Illegal Activities

No UCPS-owned computer systems may be knowingly used for activities that are considered illegal under local, state, federal, international, or other applicable laws. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning.
- Unauthorized Network Hacking.
- Unauthorized Packet Sniffing.
- Unauthorized Packet Spoofing.
- Unauthorized Denial of Service.
- Unauthorized Wireless Hacking.
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system.
- Acts of Terrorism.
- Identity Theft.
- Spying.
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material.
- Downloading, storing, or distributing copyrighted material.

UCPS will take all necessary steps to report and prosecute any violations of these guidelines.

Applicability of Other Policies

This document is part of a cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Audits

UCPS must conduct periodic reviews to ensure guideline compliance. A sampling of users must be taken and audited against these guidelines on a yearly basis.

Enforcement

The CTO and/or Executive Team will enforce these guidelines. Violations may result in disciplinary action, which may include suspension, restriction of access, or other punishments deemed appropriate by UCPS district personnel. Where illegal activities or theft of district property (physical or intellectual) are suspected, UCPS may report such activities to the applicable authorities.

Revision History

Revision 1.0, 8/21/2012

Revision 2.0, 10/03/2013

Revision 2.1, 11/04/2013

Revision 2.2, 11/05/2013

Revision 3.0, 7/17/2018

Revision 4.0, 6/9/2021