UCPS

UNION COUNTY PUBLIC SCHOOLS

TECHNOLOGY **SERVICES**

STAY CONNECTED

www.ucps.k12.nc.us

TABLE OF CONTENTS

UCPS 1:1 Handbook and Technology Reference

UCPS Technology Services

Dear Parent/ Guardian,

Union County Public Schools believes that today's students are true digital natives who are accustomed to instant access to information. UCPS provides access to digital content, learning tools and a Chromebook for each student in grades 3-12 who are participating in our one-to-one access model. We are offering this Chromebook based framework and appreciate your support in helping us educate children on how to maintain and utilize technology appropriately. Several of our student expectations are listed below.

The following list highlights several of our expectations for students.

SCHOOL USE **GUIDELINES:**

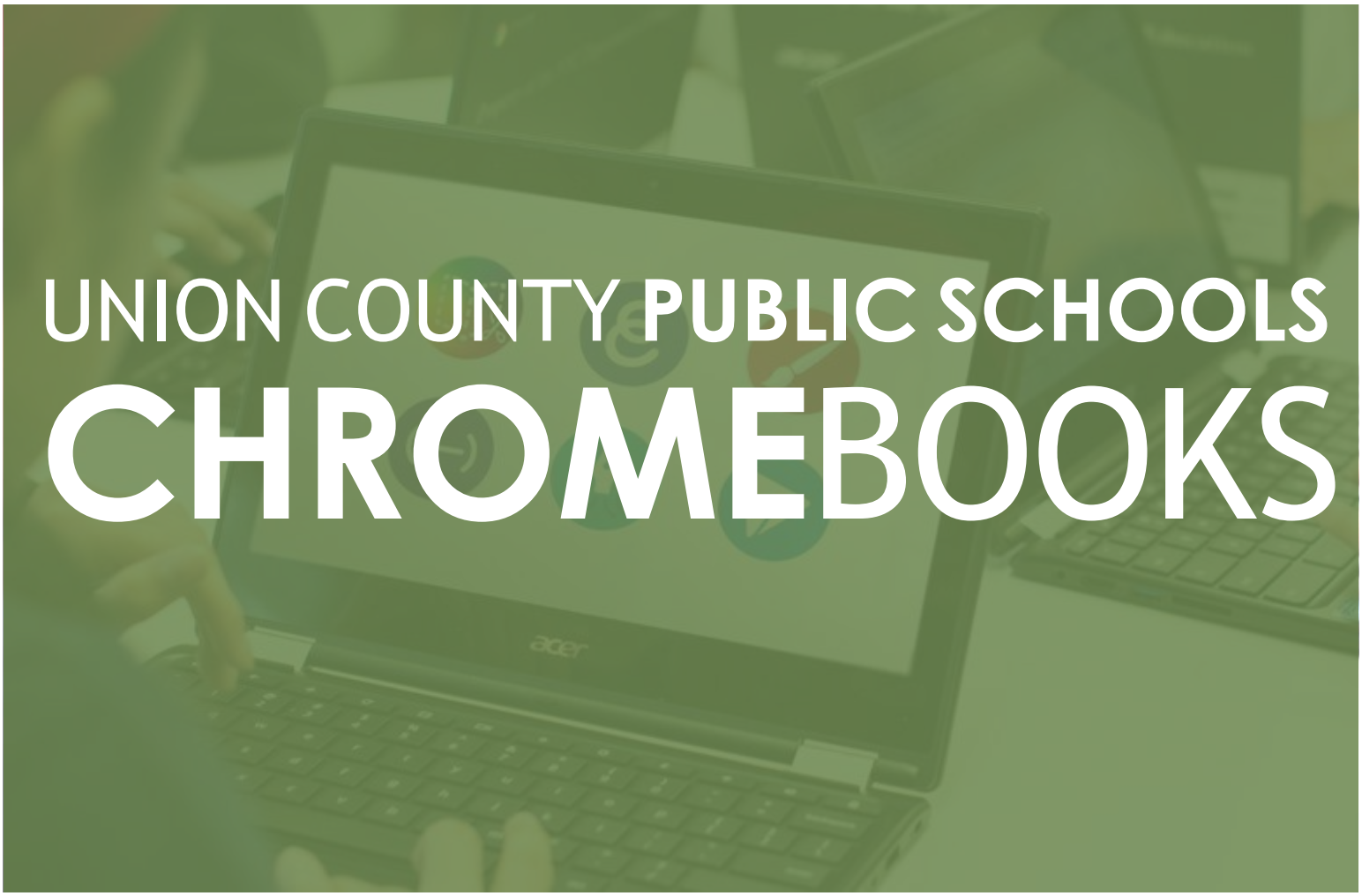
- The laptop is an educational tool and should be used in that capacity only.
- The student is the only authorized user of the assigned laptop.
- Do not eat or drink near the laptop. This includes bringing it to a lunch table!
- Do not rest pencils/pens or other items on the keyboard. Accidentally closing the laptop with items on the keyboard damages the screen.
- Cyberbullying will not be tolerated.
- Chats and emails are not private and can be accessed by approved UCPS staff.
- Students should not try to bypass the district filter in any way. This includes, but is not limited to, the use of proxy avoidance sites.

HOME USE **GUIDELINES:**

- Do not leave laptops in automobiles.
- Laptops must come to school fully charged on a daily basis.

Once again thank you for your support!

UCPS
UNION COUNTY PUBLIC SCHOOLS



UNION COUNTY PUBLIC SCHOOLS
CHROMEBOOKS

Union County Public Schools (UCPS) has chosen and approved Chromebooks for our 1:1 access model. Chromebooks are designed to be used while connected to the Internet. Rather than use traditional software that resides on the device itself, Chromebooks utilize the web-based Google Chrome Operating System to quickly boot upon startup and for overall functionality. In addition to utilizing cloud computing via the Google Apps for Education Suite, Chromebooks have an internal hard drive that student work can be saved to.

This internal hard drive provides students with some offline capabilities when a wireless connection is unavailable. Additionally, USB peripheral devices such as a wireless mouse, a Smartphone or a flash drive will work when connected to a Chromebook. Students, however, will not be able to install software or run executable files; these safeguards accompany many other advanced security features.

TECHNOLOGY SERVICES

INFORMATION AND TECHNOLOGY ESSENTIAL STANDARDS

The Digital Teaching and Learning Standards are integrated into your child's daily learning experiences. These standards are divided into four key skills that are fundamental in preparing students to be successful.

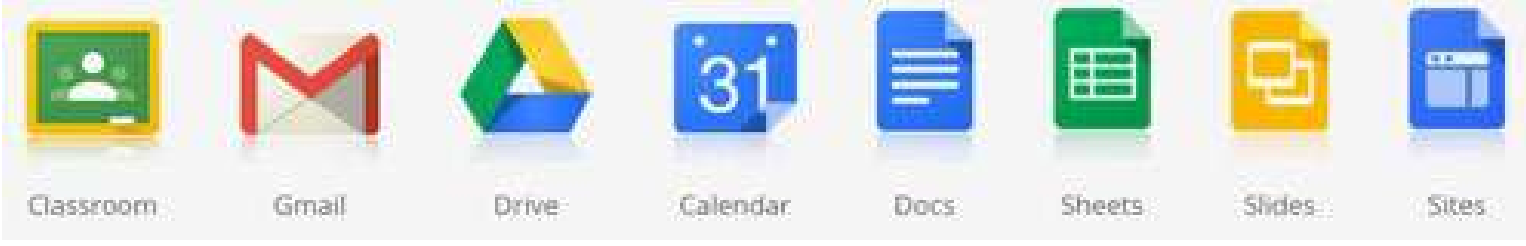
THESE KEY SKILLS INCLUDE:

- K-12 Digital Standard for Student Learning
- Digital Learning Competencies for Educators
- Professional Standards
- Additional partnerships and Resources

GOOGLE APPS **EDUCATION SUITE**

Students have access to Google Apps for Education (GAFE), an online suite of productivity tools. Teachers and students are provided GAFE accounts with varying levels of rights. GAFE allows users to create and share collaborative presentations, documents, spreadsheets and drawings. These items are created and housed within our UCPS domain.

Additionally, access to GAFE's internal email system is reserved for students in grades 6-12. Student email is limited to communicating with teachers and other students within the UCPS domain; personal and outside emails are restricted. Elementary students **DO NOT** have email access.



DIGITAL **RESOURCES**

Your child will benefit greatly from the resources provided by Union County Public Schools. In addition to the Google Apps for Education productivity suite, students will have access to a variety of UCPS supported database subscriptions such as Microsoft 0365 and One Drive.

These resources are vetted by a team of curriculum and instructional technology members and meet the specific curriculum and technology needs of elementary, middle and high school students.

You can explore these resources by visiting the appropriate student startup page:

- UCPS Student Start Up Page (Elementary)
- UCPS Student Start Up Page (Middle)
- UCPS Student Start Up Page (High)

STUDENT **APPS LOCKER**

Another resource that students will have access to is the Union County Student Apps Locker.

This resource contains approved Chromebook applications that have been vetted by both the Technology and Curriculum Departments to address student instructional needs.

UCPS STUDENT **EXPECTATIONS**

Computing expectations for student use have been outlined in the UCPS Acceptable Use Guidelines (AUG). A copy of these guidelines can be located in the resources section of this handbook as well as the UCPS website for review at any time. Each time a student logs into any UCPS computer they are agreeing to all guidelines stated within the AUG. Each year students will complete the UCPS Internet Safety and Chromebook care training.

INTERNET **SAFETY**

The Internet enhances learning by giving students access to educational information and a variety of interactive online tools. We can receive feedback from teachers, collaborate with peers, or even teach others something new. This is what makes the Internet a powerful educational resource. There are things we need to know in order to stay safe while online. We will teach your child how to navigate the World Wide Web safely and responsibly, but keep in mind that children need to have the same safety measures in place at home.

Union County Public Schools has safeguards in place to protect your child. UCPS complies with the filtering requirements mandated by the Children's Internet Protection Act (CIPA) and Children's Online Privacy Protection Act (COPPA). UCPS implements a commercial grade internet filter on ALL UCPS computers 24 hours a day, 7 days a week, 365 days a year. This protection is in place at home, school, or any other location. No filtering system is perfect but we can monitor closely and block inappropriate content. However, thousands of new sites are created daily and our filter may not catch all of them. If your child comes across inappropriate content encourage them report it to school personnel and the site will be blocked. Keep in mind that parents and guardians are the best resource when it comes to monitoring their child's online behavior.

SOCIAL **MEDIA**

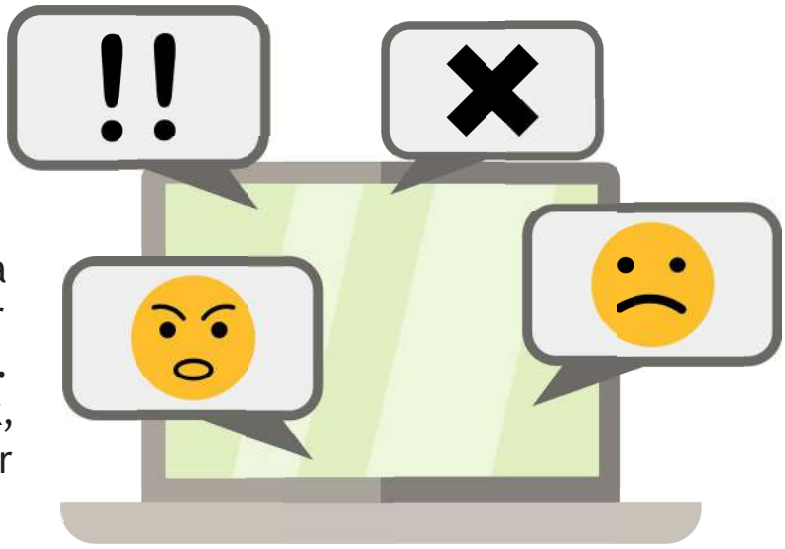
UCPS DOES NOT support or endorse social networks beyond Canvas and Google Apps for Education. A social networking site is a website that allows you to build a profile and connect with others.

Most social networking sites such as Facebook, Instagram, and Twitter are blocked for students, but as a parent it is important to be aware of them.

CYBERBULLYING

Cyberbullying is defined as using technology such as the Internet or cell phones to bully or harass someone. Here are some tips that you can utilize to help protect your child against cyberbullying:

- Know your child's username and passwords for all social networking sites.
- All social networking sites have a minimum age limit listed in their terms of service or privacy policy. Most of these, including Facebook, state that they are not intended for individuals under the age of 13.



- Friend or follow your child and monitor activity on a routine basis.

INTERNET SAFETY **RESOURCES FOR PARENTS**

CENTER for Cyber Safety™ & Education

common sense media®

TECHNOLOGY **FEE**

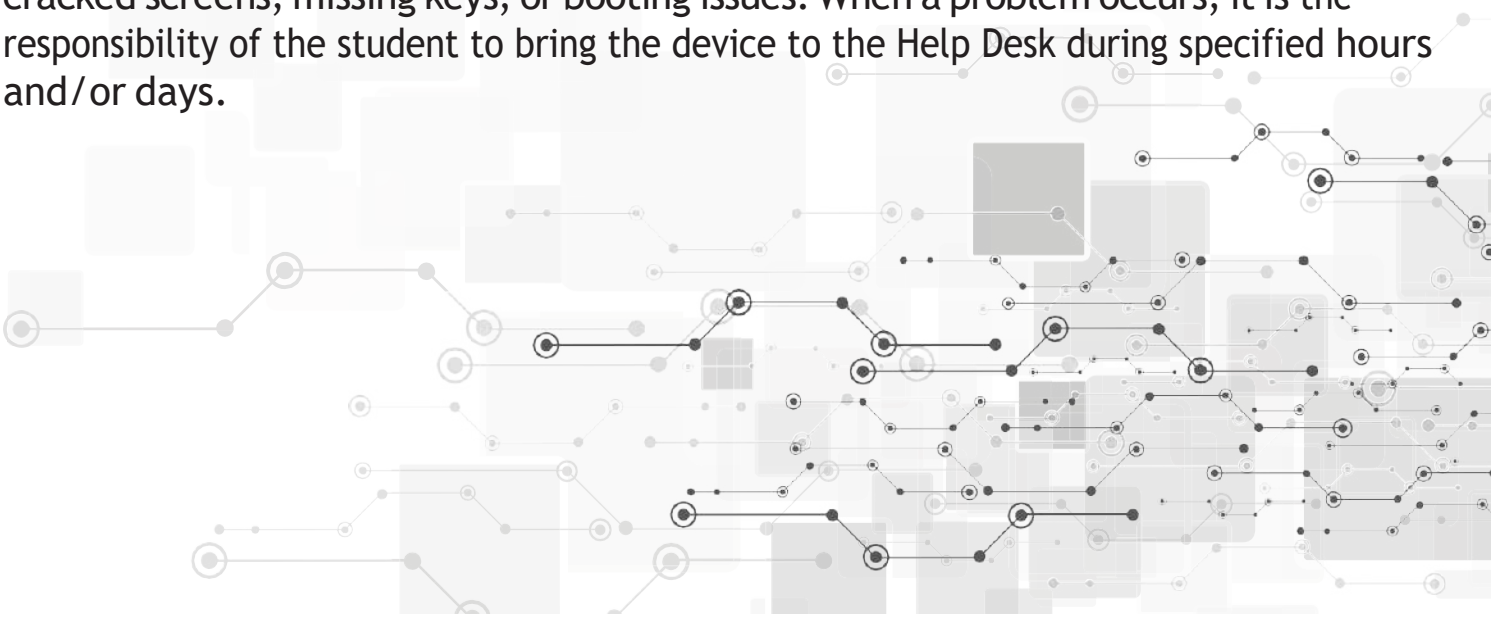
The Union County Board of Education supports a $30 annual user fee with limited accidental insurance coverage, per 3-12 grade student. This will guarantee your child's access to the most robust technology available to enhance their individualized learning while providing resources for any necessary repairs.

HOME CARE AND MAINTENANCE

It is the expectation that students care for their UCPS issued Chromebook as if it were their own, keeping it in good working condition. Students are also expected to bring their computer with them to school every day, fully charged. Even though the device has a 6-hour battery life it is the student's responsibility to charge it **EACH NIGHT**. Parents can reinforce this behavior at home.

It is required that the UCPS issued Chromebook be carried in a protective case that is provided. If cases are removed, this may void the accidental damage insurance coverage. Avoid placing anything heavy on top of the device as this may damage the screen. Also keep food and liquids away from the device.

If your child happens to experience any issues with their Chromebook, charger, or any application on it, each school has resources to help troubleshoot the problem. Each school has been assigned a Support Engineer to assist with hardware issues such as cracked screens, missing keys, or booting issues. When a problem occurs, it is the responsibility of the student to bring the device to the Help Desk during specified hours and/or days.



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, or Cyberbullying. 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 provided storage should be utilized when possible, such as Microsoft One Drive or Google Cloud.
- 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 very risky 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.

STREAMING **MEDIA**

Streaming media can use a great deal of network resources and is controlled and managed by district firewall configurations.

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. Daily monitoring of activities and compliance software may be used to manage this resource.

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 the System Administrator.

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 Technology Services.

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.
- Installation of malicious software.

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 may be taken and audited against these guidelines as needed.

ENFORCEMENT

The CTO and/or Executive Team members 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.