Wayland-Cohocton Central School District
Acceptable Use Policy and Rules (AUP)
for Technology Access for Non-Students

Introduction

The Wayland-Cohocton Central School District (WCCS) Information Technology Department Acceptable Use Policy and Rules for Technology Access for Non-Students exists to guide the conduct of the non-student when on a WCCS campus or using WCCS technology as it pertains to technology resources. It is not intended to replace in part, or in whole, pertinent New York or federal laws. Such laws include, but are not limited to the Family Educational Rights and Privacy Act (FERPA, 20 USC § 1232g); the Health Insurance Portability and Accountability Act (HIPAA, Pub.L. 104-191); the Children's Internet Protection Act (CIPA, 47 USC § 254); the Children's Online Privacy Protection Act (COPPA, 15 USC § 91); the New York State Penal Law, Article 156; the Public Records Law; the Digital Millennium Copyright Act; the Computer Fraud and Abuse Act of 1986 (CFAA, 18 USC § 1030); the Computer Abuse Amendments Act of 1994; or obscenity and child pornography laws; NYS Freedom of Information Law (FOIL, NY Pub. Off. Law § 84) and the Digital Millennium Copyright Act (DMCA, 17 USC § 1201). In the event that this Policy conflicts with any of the aforementioned statutes and regulations, that statute and/or regulation will control.

In the event that any handbook distributed by the District or one of the schools of the district conflicts with this AUP, this AUP will control.

Non-students with access to the District's network agree to comply with the WCCS Acceptable Use Policy and Rules for Technology Access with applicable state and federal laws dealing with appropriate, responsible and ethical use of information technology. Non-students include instructional and non-instructional staff, school administration, members of the Board of Education, vendors and other guest users. Students have their own Acceptable Use Policy binding their use of District technology and network.

It is the responsibility of the non-student to be aware of the existing policies and to adhere to their guidelines. Non-compliance is a serious breach of the Wayland-Cohocton Central School District's standards and may result in legal and/or disciplinary action for all staff, employees and students. This Acceptable Use Policy and Rules for Technology Access (AUP) outline the guidelines that all non-students are expected to follow when using school technology resources or when using personally-owned devices on the school campus.

It is a general policy that the network/Internet will be used in a responsible, efficient, ethical, and legal manner in accordance with the WCCS District Mission. The network is not a public access service or a public forum. Failure to adhere to the AUP may result in suspending or revoking the offender's privilege of access. Any adult who uses the WCCS network must sign the Contract at the end of this AUP before they are allowed to use the WCCS Networks.

Data Security Officer

The designated WCCS Data Security Officer is the Superintendent of WCCS. The role of the Officer is to monitor the District's data security program and to have oversight of compliance with regulations, security policies, standards and guidelines. The Officer is responsible for coordinating and executing the District's security program and functions as a technology liaison to the District's students and non-students. The Officer also ensures all non-students are educated as to how to operate technology effectively and within the policies of this AUP.

Technology Resources Covered

WCCS may offer the privilege of Internet access, desktop computers, mobile computers or devices, whiteboards, videoconferencing capabilities, online collaboration capabilities, Internet forums, email, and other forms of electronic technology and communication to non-students. This AUP applies to school-owned technology resources and the use of the WCCS network at any time, the use of the WCCS Internet connection, and/or the use of private networks and Internet connections with or through school-owned technology. This AUP also applies to privately-owned devices accessing the WCCS network, the WCCS Internet connection, and/or private networks and Internet connections while on school property. The Policies and Rules outlined in this document apply to all available technologies now and into the future, not just those specifically listed or currently available.

Usage Policies

All technology resources provided by the District are intended for educational purposes. Acceptable uses of the network are activities which support learning and teaching. Incidental personal use of electronic resources is permissible but must not adversely affect the performance of employee's official duties or the organization's work performance, must not be disruptive of co-workers or students, must be of limited duration and frequency, should be restricted to matters that cannot be addressed during non-duty hours, and must not violate any other provisions of this Policy. Incidental use may not jeopardize the safety, security, effectiveness or usefulness of the District's technology resources.

● User Accounts

All Accounts

The District grants the privilege of a network account to complete tasks related to their job responsibilities to, among others, faculty and staff, school administration, members of the Board of Education, vendors and other guest users. This account grants access to log into WCCS technology resources.
Each non-student will be given a username and will be prompted to change their initial password that meets the following minimum complexity requirements:

Password Requirements:

✓ Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
✓ Passwords must be at least eight characters in length or the number of characters specified in the Minimum password length policy setting.
✓ Passwords must contain characters from at least three of the following four categories:

- English uppercase alphabet characters (A–Z)
- English lowercase alphabet characters (a–z)
- Base 10 digits (0–9)
- Non-alphanumeric characters (for example, !$#,%)
- Enforced by server policy, user passwords will expire every 90 days and must be changed.

Guest users

Guest users will be provided access to a guest wireless session for limited and filtered Internet access. Tampering with this filter in any way may result in immediate revocation of IT privileges and penalties.

Termination

When employment with WCCS terminates, or duties are changed, the user account must be deleted, disabled, or changed. The Administration must fill out an Employee Status Form for Leave of Absence, Transfer, Resignation, Retirement or Termination to be initiated by the Superintendent's Secretary. Upon termination of employment, departing employees are prohibited from archiving or removing electronic or written files without Information Technology Department or Administrative permission.

● Web Access

It should be assumed that all web browsing is monitored and reviewed at all times, and web activity records may be retained indefinitely. Browsing is a privilege subject to this AUP, and each and every web page visited must comply with the District's policies and rules.

Non-students are expected to respect the web filter as a safety precaution, and shall not attempt to circumvent the web filter when browsing the Internet. If a non-student believes a site is unnecessarily blocked, he or she may request a website review through the Information Technology Department, then sent for a final decision by the Data Security Officer.

● Email

Email Accounts

Upon employment, the Information Technology Department establishes email accounts for designated WCCS employees for use during active employment. After employment is terminated, the account is disabled from the email system at the direction of the Superintendent or his/her designee.

Filtering

WCCS uses Google Mail (Gmail) which has comprehensive virus and spam filtering protection. WCCS accepts no responsibility for any damage caused to personal devices by receiving emails from our email system.

Personal Use

Incidental, personal use of the email system is permitted; however, the personal use must not interfere with the employee's work or the work of others, and must not be prohibited by this policy or any federal, state or local law, statute, ordinance, rule or regulation.

Public Records

Email which is created or received by a WCCS employee in connection with the transaction of official business of the WCCS will be considered a public record, property of WCCS, may be subject to inspection and/or copying in accordance with NYS FOIL. Email use on District property is not to be construed as private.

Archival and Retention

Retention of email messages are covered by the same retention schedules as records in other formats, but are of a similar program function or activity. Email shall be maintained in accordance with the NYS Records Retention and Disposition Schedule ED-1 as outlined in the Records Management Policy. Email records may consequently be deleted, purged or destroyed after they have been retained for the requisite time period established in the ED-1 schedule. All email sent and received to an employee's email account shall be archived by the District for a period of no less than six (6) years. This time period was determined based on the possibility of emails that are the official copy of a record according to schedule ED-1.

Prohibited Uses of Email

The WCCS email system shall not be used for any unauthorized purpose including, but not limited to:

a. Sending solicitations including, but not limited to, advertising the sale or receipt of goods or services for personal gain or other commercial activities, which have not been approved by WCCS.

b. Sending copies of documents in violation of copyright laws or licensing agreements.

c. Sending information or material prohibited or restricted by government security laws or regulations.

d. Sending information or material which adversely affects the WCCS ability to carry out its mission.

e. Sending information or material which may be perceived as representing the WCCS official position on any matter when authority to disseminate such information has not been expressly granted.

f. Sending confidential or proprietary information or data to persons not authorized to receive such information, either within or outside the WCCS.

g. Sending messages or requesting information or material that is fraudulent, harassing, obscene, offensive, discriminatory, lewd, sexually suggestive, sexually explicit, pornographic, intimidating, defamatory, derogatory, violent or which contains profanity or vulgarity, regardless of intent. Among those which are considered offensive include, but are not limited to, messages containing jokes, slurs, epithets, pictures, caricatures, or other material demonstrating animosity, hatred, disdain or contempt for a person or group of people because of race, color, age, national origin, gender, religious or political beliefs, marital status, disability, sexual orientation or any other classification protected by law.

h. Sending messages or requesting information reflecting or containing chain letters or any illegal activity, including, but not limited to gambling.

i. Sending or requesting information or material that proselytizes or promotes a religious or political view, cause, position or action.

j. Sending Spam. Spam is any unsolicited email message sent to a large number of people. Typically this includes cases where:

- •The recipient did not request the message.
- •The recipient does not know the sender.
- •Bulk mailing lists are used to send unsolicited marketing or sales information.

Sanctions

The Information Technology Department may report inappropriate use of email to the Superintendent, who will take appropriate disciplinary action. Violations may result in a loss of email use, access to the technology network and/or other disciplinary action. When applicable, law enforcement agencies or collective bargaining units may be involved.

Confidentiality Notice

Email messages sent from users of the WCCS email system adheres to the following disclaimer:
"Confidentiality Notice: The information contained in this electronic message is intended for the exclusive use of the individual or entity named above and may contain privileged or confidential information. If the reader of this message is not the intended recipient or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that dissemination, distribution or copying of this information is prohibited. If you have received this communication in error, please notify the sender immediately by telephone and destroy the copies you received."

● Social Collaboration

Recognizing the benefits that collaboration brings to education, WCCS may provide access to web sites or tools that allow communication, collaboration, sharing, and messaging among users subject to this AUP. Posts, chats, sharing, and messaging may be monitored. Non-students should be careful not to share anyone's personally identifiable information online (see below, "Personal Information")

● Social Media

Teachers may upload homework, post school notices, moderate discussions and share materials, with the understood prohibition against sharing any student's personally identifiable information.

Mobile Devices Policy

WCCS may provide non-students with District-owned mobile computers or other devices outside of the classroom. Users of those devices are subject to this AUP, the 1:1 Chromebook Policy and Guidelines, when using school devices off the school network as well as on the school network. Users of these devices are expected to treat these devices with extreme care and caution. Users of these devices should immediately report any loss, damage, or malfunction to the Information Technology Department; users of these devices may be financially responsible for any damage resulting from negligence or misuse.

Personally-Owned Devices Policy

WCCS does not allow personally owned devices on the District network.

Cell phones used by staff that access District email are expected to have lock codes enabled for security protection of school email/data. In order to access the WCCS wireless network, staff must comply with the AUP. If a cell phone is lost or stolen, the non-student is required to report the loss or theft to the Information Technology Department for school email/data deactivation.

WCCS is not liable for the loss, damage, misuse, or theft of personally owned devices brought to school. Any purposeful interference on behalf of a student or a non-student with an investigation by the District into possible violations will be considered a violation of equal gravity.

Security

Non-students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a District-provided computer or mobile device you are using might be infected with malicious software (e.g., virus, spyware, malware, adware, etc.), you must cease using it and immediately notify the Information Technology Department. Do not attempt to remove the malicious software yourself or download any programs to help remove it.

Software Downloads

Non-students should not download or attempt to download or install software programs through the school network or on school technology resources without express permission from the Information Technology Department staff. You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Netiquette

Non-students should always use the Internet, network resources, and online sites in a manner that is in accordance with this AUP and Rules. The District has a right to place reasonable restrictions on the material accessed and posted by non-students through the system. Non-students may not use the network to offer, provide or advertise products or services through the network. Non-students may not use the network for gambling, and may only use the network for fundraising with express written permission from school administration.

Non-students should remember not to post anything online that they would not want others to see. Once something is online, permanence should be assumed, leaving a digital footprint that can be tracked, shared and spread in ways never intended.

Non-students are prohibited from knowingly transmitting or accessing, on or through the network, any material that is unlawful, profane, discriminatory, sexually oriented, obscene, threatening, abusive, harassing, libelous or hateful, or that encourages in any way conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state or Federal law. A limited exception will be made for accessing such material if it is for a legitimate educational purpose, and school administration must be notified in advance and be able to fully monitor such activity at will.

The District reserves the right to remove material protected by copyright, trademark, trade secret or any local, state or Federal law from the network.

Personal Information

In accordance with FERPA, HIPAA and NYS Education Law 2-d, regarding personally identifiable information (PII), staff should never disclose or share their own or anyone else's personal information, particularly students. No such information should be broadcasted or published in any way from the District network or devices. If there is a question as to whether sending communications would violate this mandate, consult the Information Technology Department immediately. PII includes:

1) Any phone number;
2) Address of individual or family;
3) Social security number or other identification number;
4) Date of birth;
5) Any health information, biometric record or information about medical care or treatment;
6) Any financial information; or
7) Anything that may be considered harmful or embarrassing to an individual if disclosed alone or in combination with certain other information. Users should recognize that communicating over the Internet brings perceived anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.

No Expectation of Privacy

Data files and electronic storage areas shall remain District property. There can be, and there is, no expectation of privacy with respect to a non-student's use of the District's technology resources, including the District's network and Internet access. The District retains the right to review, monitor and retain information relating to staff use of school technology resources as well as the District network and Internet access for any reason, including, assuring compliance with applicable laws, rules and regulations, as well as compliance with the Acceptable Use Policy and Rules for Technology Access. This includes accessing and reviewing current use, stored information, logs of incoming and outgoing information, communications using the District network and Internet access, and all of its content. Assume at all times that the monitoring and review is occurring.

Limitation of Liability

WCCS will not be responsible for damage or harm to a staff's personal technology devices, software or data, including but not limited to cell phones, smart phones, files, data, or hardware. WCCS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network or using the school Internet access. The privilege of use may be revoked at any time by the District without notice, and the District is not responsible for data or information lost in this process.

Receipt of Acknowledgment

The below signature of acknowledgment is required by non-students to use the District's technology, including the network. The privilege of use may be revoked at any time by the District without notice, and the District is not responsible for data or information lost in this process.

By signing below, I hereby acknowledge receipt of the Wayland-Cohocton Central School District Staff Acceptable Use Policy and Rules for Technology Access. I understand it is my responsibility to review the Policy and Rules, and request any clarification needed from the Information Technology Department staff or the Data Security Officer.

By signing below, I agree to comply with this AUP. I understand that violation of any policies, procedures and standards shall be grounds for loss of access to technology resources and/or disciplinary proceedings.

I also understand this signed acknowledgment of receipt will be kept on record by the District; and for staff members, the acknowledgment will become a permanent part of personnel files, and a copy will be kept in the Information Technology Department for establishing staff user accounts.

I acknowledge receipt of this AUP in hard copy form. In addition, I have access to District webpage link to Policies for Technology Use (http://www.wccsk12.org/sites/wccsk12.org/files/files/AUPNon-Student.pdf). I have read, understand and will abide by the policies stated in the Wayland-Cohocton Central School District Non-Student Acceptable Use Policy and Rules for Technology Access.

By signing below, I agree to **not give anyone else access** to the District's technology or network without their compliance with this AUP. I understand that failure to comply with these terms and conditions may result in the loss of my access to the network, and may result in imposition of penalties under local, state or Federal law, or under a collective bargaining agreement if involved. I agree to immediately report all student or non-student violations of the District's Information Technology policies to District officials and the Data Security Officer.

Wayland-Cohocton Central School District

Acceptable Use Policy and Rules (AUP) for Technology Access for Non-Students Contract

AGREEMENT

I understand and will abide by the above terms and conditions for use of the District's technology and network. I understand that failure to comply with these terms and conditions may result in the loss of my access to the District's technology and network and may, in addition, result in the imposition of penalties under a collective bargaining agreement, if any, or federal, state or local law. **I shall report all violations of the District's policies to the Information Technology Department or the Superintendent.**

Print Name _____

Position Title/Building/Department _____

Principal/Supervisor _____

Non-Student Signature _____ Date _____

Revised: October 22, 2015