Wilmington City Schools

Acceptable Use Policy and Internet Safety Agreement
2018- 2019

Statement of Purpose

Wilmington City Schools is pleased to offer our students' access to the World Wide Web and other electronic networks. The advantages afforded by the rich, digital resources available today through the World Wide Web outweigh any disadvantage. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved.

Terms of Agreement

In order for a student to be allowed access to a school computer system, computer network, and the Internet, parents must sign and return the attached consent form by **8/24/2018**.

Acceptable Uses

Use of the District's electronic resources by staff, students, and/or visitors to the District in an illegal or unethical manner may result in disciplinary action, including loss of privileges to use the system, school or District sanctions, and referral to appropriate law enforcement authorities. Users may be required to make full financial restitution. The District is providing access to its school computer systems, computer networks, and the Internet for educational purposes only. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide. Accordingly, regulations for participation by anyone on the Internet shall include, but not be limited to the following:

- All users must abide by rules of Network etiquette — Netiquette, including the following:
    - Be polite. Use appropriate language and graphics. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
    - Avoid language and/or graphic representations which may be offensive to other users.
    - Don't use network or Internet access to make, distribute, or redistribute jokes, stories, or other material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
    - Do not assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
    - Teachers may allow individual students to use e-mail, electronic chat rooms, instant messaging, social networking sites (i.e., face book and Instagram) and other forms of direct electronic communications **for educational purposes only** and with proper supervision. Proper supervision shall include the teachers having the documentation of the students' username and password on file and being able to monitor the account. This includes the use of student personal e-mail accounts and personal social networking sites in the school environment. If a student uses his/her personal e-mail account or accesses his/her social networking site on a school computer, the teacher must monitor all communications and have access to the student's username password for such account.
- No personal addresses, personal phone numbers, or last names of students will be permitted to be given out on the Internet. No identifiable photographs will be allowed to be published on the Internet without appropriate written consent. Concerning a student, appropriate written consent means a signature by a parent or legal guardian of the student.
- A student may not attempt to access any Internet resource without the prior consent of the teacher. The Internet is an extension of the classroom and teachers are responsible for and must be aware of where their students go on the Internet.

System Security

- System logins or accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account
- Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any entity on the K through 12 Network.

Privacy

Network and Internet access is provided as a tool for education. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District and no user shall have any expectation of privacy regarding such materials.

Copyright

All students and faculty must adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information.

Failure to Follow Acceptable Use Policy

Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network and Internet terminated and is subject to disciplinary action by the school administrator. The District may also take other disciplinary actions.

Unacceptable Uses of the Network may include the following:

- Uses that cause harm to others or damage to their property. For example, do not engage in defamation (harming another's reputation by lies); do not employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; do not upload a work, virus, Trojan horse, time bomb, or other harmful forms of programming or vandalism; do not participate in hacking activities or any form of unauthorized access to other computers, networks, or information systems.
- Uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, do not disclose or share your password with others; do not impersonate another user.
- Uses that are commercial transactions. Students may not use the school network to sell or buy anything over the Internet. You should not give others private information about yourself or others.
- Illegal activities, including copyright or contract violations shall not be permitted on the Internet.
- The Internet shall not be used for commercial, political, illegal, financial, or religious purposes. Violations shall be reported to a teacher or an administrator immediately.
- Threatening, profane, harassing, or abusive language shall be forbidden.
- Use of the network for any illegal activities is prohibited. Illegal activities include (a) tampering with computer hardware or software, (b) unauthorized entry into computers and files (hacking), (c) knowledgeable vandalism or destruction of equipment, and (d) deletion of computer files. Such activity is considered a crime under state and federal law. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
- No user is permitted to knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system. No third party software will be installed without the consent of the assigned administrator.

- Invading the privacy of another user, using another's account, posting personal messages without the author's consent, and sending or posting anonymous messages shall be forbidden.
- Accessing pornographic or obscene materials or using or sending profanity in messages shall be forbidden.
- Any subscription to list serves, bulletin boards, or on-line services shall be approved by the superintendent or his designee prior to any such usage.
- The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

Internet Safety

- Parents and Users: Despite every effort for supervision and filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
- Personal Safety: In using the network and Internet, users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet without a parent's permission.
- Confidentiality of Student Information: Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.
- Active Restriction Measures: The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The use of anonymous proxies to get around the content filter is strictly prohibited and will be considered a violation of this policy. The school will also monitor the online activities of students, through direct observation and/or technological means.

Use of Web Tools

Online communication is critical to our students' learning of 21st Century Skills and tools such as blogging and podcasting offer an authentic, real-world vehicle for student expression. Again, as educators, our primary responsibility to students is their safety. Hence, expectations for classroom blog, student protected e-mail, podcast projects or other Web interactive use must follow all established Internet safety guidelines.

Blogging/Podcasting Terms and Conditions:

- Web 2.0 tools (i.e. blogs, wikis) may be utilized as an extension of the classroom. Whether at home or in school, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, or other Web 2.0 tools. Comments made on school related blogs should follow the rules of online etiquette detailed above and will be monitored by school personnel. If inappropriate, they will be deleted and disciplinary consequences may apply.
- Students using blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
- A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
- Any personal blog a student creates in class is directly linked to the class blog which is typically linked to the student profile, and therefore must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students must realize that anywhere they log in, it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and follow these guidelines. Comments made on blogs are monitored.
- Never link to websites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.

- Students using such tools agree to not share their username or password with anyone besides their teachers and parents and treat blog spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Guidelines for Student E-mail

Student access to e-mail is a privilege with a corresponding degree of responsibility for the user.
Students will be provided an e-mail account for instructional use as needed. As an instructional tool, student e-mail accounts can be monitored and controlled by the classroom teacher and /or district. This is a privilege extended to aid in learning and it may be withdrawn or modified by staff if it is misused. By signing this document to use school provided e-mail or a school computer you become responsible for your actions with these tools and are accountable for them.

Student e-mail responsibilities include but are not limited to the following:

- Students should not include personal information in their e-mail messages (name, phone number, age, home address).
- Students must not use e-mail in an inappropriate or offensive manner.
- Passwords, or other access codes or identifiers, are not to be shared by student users. No student is authorized to use any other person's username, password or e-mail account.

Privately Owned Electronic Devices

Students are permitted to bring privately owned electronic devices *only when given the specific permission to do so by a teacher or principal*. Students who would like to use privately owned laptops are required to have the laptop periodically evaluated by the Director of Technology.

Privately owned laptops with wireless or Ethernet connectivity will not be allowed access to the network if file sharing software is installed on the hard drive (ex. KaZaA, Morpheus, Limewire, etc). Students are responsible for the maintenance and security of privately owned laptop and all other electronic devices. The district cannot be held liable for the damage or theft of privately owned property, this includes damages resulting from computer viruses.

The district requires that privately owned laptops have operable anti-virus software installed with recent virus definition updates. Students must first meet with the Director of Technology to review these policies and receive a clean bill of health for their laptop along with a sticker that must be kept on the laptop throughout the school year. All applicable sections of this agreement apply to privately owned laptops used on school grounds.

Any damages incurred to personally owned devices as a result of use on the Wilmington City Schools Network are the responsibility of the owner. The privacy and security of any item stored on or transmitted by personally owned devices is the responsibility of the owner.

For all privately owned computing or technology devices approved and used within Wilmington City Schools, the District reserves the right to:

- Monitor and log all activity.
- Determine when and where the use of such devices is permissible.
- Determine whether specific uses of these devices are consistent with the Acceptable Use Policy and Discipline Handbook.
- Determine whether use of these devices or network resources is appropriate.
- Remove the user's access to the network and/or terminate the right to use personally owned equipment in district facilities if it is determined that the user has engaged in unauthorized activity or has violated the Acceptable Use Policy.

Teacher Responsibilities

- Will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the district curriculum.
- All students will be informed of their rights and responsibilities as users of the district network prior to gaining access to that network, either as an individual user or as a member of a class or group.
- Use of networked resources will be in support of educational goals.
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy.
- Provide alternate activities for students who do not have permission to use the internet.

Principal Responsibilities

- Be sure handbooks are distributed to all students.
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy.
- Permission forms must be kept on file for one year.
- Students who do not have permission to use the internet must be identified to the teaching staff.

District Responsibilities

- Ensure that filtering software is in use to block access to materials that are inappropriate, offensive, obscene, or contain pornography.
- Have Acceptable Use Policy approved by the board and reviewed yearly.

Additional information regarding additional student expectations are spelled out in the student handbook.

Wilmington City Schools

Acceptable Use Policy, Internet Safety Agreement, and Google Chrome Book Student Agreement

Parent/Guardian Consent

Please detach the Acceptable Use Policy and only return this Agreement Form.

Child's Name: _____ Grade: _____

As a parent or legal guardian of the child named above, I have read and understand the Acceptable Use Policy and Internet Safety Agreement and I agree to the following:

(Please circle YES or NO for each item)

YES NO I grant permission for my son or daughter to use a **school computer and software** provided by WCS, provided my child follows the terms described in the district's Acceptable Use Policy.

YES NO I grant permission for my son or daughter to **access the Internet** services provided by WC S, provided my child follows the terms described in the district's Acceptable Use Policy.

YES NO I acknowledge and understand my obligations as outlined in the Google Chromebook Student Agreement for my son or daughter to use a **school Chromebook and software** provided by WCS.

_____

Parent Name (printed) Parent Signature Date

Student Agreement

I have read or had explained to me the district's Acceptable Use Policy, Internet Safety Agreement, and Google Chrome Book Student Agreement. I understand and agree to follow these terms. I understand that if at any time I do not comply with these terms I may be subject to loss of Internet or computer privileges or other disciplinary measures.

_____

Student Name (printed) Student Signature Date

This form is due by ***Friday, August 24, 2018***

Asset Tag #_____

S/N#_____