Cincinnati Public Schools

Student Acceptable Use Policy and Internet/Network Safety Agreement
Cincinnati Public Schools 2017-2018 School Year

Students will digitally sign a grade-appropriate version of this Acceptable Use Policy (AUP) and the Internet/Network Safety Agreement at school through a link provided in Schoology.

Statement of Purpose - The purpose of providing technology devices and Internet and network access in schools is to support the District's educational objectives.

Terms of Agreement - To be allowed access to school computer systems, computer networks, software applications, including Google Applications for Education, and the Internet, students must read a grade-appropriate version of this agreement and sign the consent form. **Students will digitally sign the consent forms at school**.

Parents, please read this document so that you are familiar with CPS' policy.

Rules for Internet/Network Usage -
The district is providing access to its school computer systems, computer networks, district-adopted tools and devices, software applications, including Google Applications for Education, and the Internet for **educational purposes only**, including accessing and sharing information with teachers and other students, storing files, conducting research, and collaborating on projects with others. If you have any doubt about whether a contemplated activity is educational, consult with the principal or teacher assigned to assist you. Use of the district's network and Internet is a privilege.

A user who violates this agreement shall, at a minimum, have access to the network and Internet terminated and is subject to additional disciplinary action based on the severity of the violation. All users are bound by the Cincinnati Public Schools (CPS) Code of Conduct and the following terms and conditions:

Student Safety/Education

Cyber-bullying

Cyber-bullying means any intentional, electronically transmitted (including the use of text messaging, instant messaging, or the posting of text or images) verbal or graphic act that a student or group of students repeatedly exhibit toward another student(s) and the behavior causes mental harm (including humiliation and embarrassment) and is sufficiently severe, persistent or pervasive.

Any cyber-bullying, harassment or intimidation is strictly prohibited. If a student is found to have engaged in cyber-bullying, disciplinary action will be recommended. If a student thinks that he or she is the victim of cyber-bullying, the situation should be immediately reported to an adult staff

member, such as a teacher or principal. Additionally, students are encouraged to notify school staff if they suspect another student is being cyber-bullied.

Sexting

Sexting is the sending of sexually explicit images through any electronic media, including but not limited to text messaging, instant messaging, or email. **Sexting is strictly prohibited** and is considered a Category III offense in CPS' Code of Conduct. Sexting should be immediately reported to an adult staff member, such as a teacher or principal.

Depictions of Prohibited Conduct

- Never make, reproduce or distribute videos, images, sound recording or other mediums that show behavior prohibited by the Code of Conduct on school property or at school events, including using school-owned or personal electronic devices.
- Never post depictions of prohibited behavior on social networking sites such as Facebook, Google Plus, YouTube, Instagram, Snapchat or any other similar Web sites.
- Any depictions of prohibited behavior must be immediately turned over to the principal.

Social Networks/Chat Rooms

- Never post personal information, such as full name, Social Security number, address, telephone number, bank or credit card numbers, etc.
- Consider not posting photographs of yourself. Never post sensitive or inappropriate photos. If you do post a photo, consider whether it is a photo that your mother would display in the living room.
- Assume that everything you post is on the Internet permanently.
- Do not agree to meet in person someone you know only from a social networking site or chat room.

Basic Internet/Network Etiquette & Safety Rules

- The CPS Code of Conduct and district policies on "Plagiarism/Cheating," "Bullying and Other Forms of Aggressive Behavior," and "Bullying – Harassment – Intimidation — Sexting" apply to Internet/network conduct.
- Gaggle will monitor and filter all student email and Google Apps content. Inappropriate or flagged messages will be blocked and sent to an administrator.
- Be polite. Use appropriate language and graphics.
- Do not use network or Internet access to make, distribute or redistribute jokes, stories or other material based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion or sexual orientation.
- Teachers may allow individual students to use email, electronic chat rooms, instant messaging, social networking sites and other forms of direct electronic communications, including Gmail and Google Hangouts, for **educational purposes only** and with proper supervision.
- **Student Photos/Student Work** - Publishing student pictures and work on websites promotes learning and collaboration, and provides opportunities to share the achievements of students. Images and products of K-12 students may be included on the website only without identifying captions or names. **Parents/guardians must indicate their written consent to publish their child's photo or school work on any school-related website before the item is published to the web.**

  Please note that under no circumstances will K-12 students' photos or work be identified with first and last names on district, school or teacher websites.

- **Privacy** - Network and Internet access is provided as a tool for your 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. Do not download copyrighted material or software without permission of the owner.
- Do not sell or buy anything over the Internet.
- Do not transmit or access obscene or pornographic material; notify your teacher if you receive such material.
- Any subscription to list serves, bulletin boards or on-line services shall be reviewed by a district administrator and must be approved by the teacher prior to any such usage.
- Do not access the network or Internet by any means or device other than those approved by the teacher.
- Do not post inappropriate speech on any blogs, podcasts, Google Applications or other web 2.0 tools.

  Such tools are considered an extension of your classroom, and any speech that is considered inappropriate in the classroom is also inappropriate in all uses of these Web tools. This includes, but is not limited to, profanity and racist, sexist or other discriminatory remarks. Comments made on blogs will be monitored and, if they are inappropriate, deleted. Any student violating this rule will be subject to disciplinary action.

- Do not use the network or Internet for any illegal activity, including (a) tampering with computer hardware, software or data, (b) unauthorized entry into computers and files (hacking/cracking), (c) knowledgeable vandalism or destruction of equipment, and (d) deletion of computer files. Such activity is considered a crime under both state and federal laws and will be disciplined accordingly.

- Do not use the network or Internet to send messages relating to or in any way supporting illegal activities such as the sale or use of drugs or alcohol; support of criminal or gang activity; threats, intimidation or harassment of any other person.

- All of the above rules expressly apply to, but are not limited to, the use of Google Applications for Education, which include, but are not limited to, Gmail, Google Drive, Google Calendar, Google Hangouts, Google Docs and Google Forms.

Network/System Security/Content Filtering

- If an Internet/network security issue is identified, the user must notify an adult, such as a teacher, who will in turn notify a system administrator. The problem should not be demonstrated to other users.
- Do not attempt to log on as a system administrator. This action will result in cancellation of privileges.
- Do not use anonymous proxies to circumvent district-implemented content filtering.
- Do not 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.
- Do not install third-party software without the consent of your assigned administrator.
- Do not share your passwords.

- **Do not use another person's accounts or passwords.**
- Technology protection measures may be disabled by an authorized person. This will be done only by Information Technology Management (ITM) during adult computer usage to enable internet access for research or other lawful purposes.
- Do not participate in hacking/cracking activities or any form of unauthorized access to other computers, networks, or information systems.

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's curriculum.
- All students will be informed of their rights and responsibilities as users of the district's 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 this AUP according to the CPS Code of Conduct.
- Provide alternate activities for students who do not have network and Internet privileges.

Principal Responsibilities

- Include this AUP in your school's Student Handbook.
- Distribute Student Handbooks to all students.
- Treat student infractions of this AUP according to the CPS Code of Conduct.
- Keep the signed Consent Forms on file for one year.
- **Identify to the teaching staff those students who do not have permission to use the Internet.**

District Responsibilities

- Ensure that filtering/blocking software is in use to block access to sites and materials that are inappropriate, offensive, obscene, contain pornography, or are otherwise harmful to minors.
- Restrict unauthorized disclosure, use and dissemination of personal information regarding minors.
- Post this AUP on the district's website.

Student Acceptable Use Policy and Internet/Network Safety Agreement Consent Form

Students will digitally sign a grade-appropriate version of this Acceptable Use Policy (AUP) and the Internet/Network Safety Agreement at school through a link provided in Schoology.

Cincinnati Public Schools reserves the right to change this policy at any time.