

***COMPUTER/NETWORK ACCEPTABLE USE POLICY***

The Hudson City School District (HCS D) is pleased to offer 21st Century Technology to their employees and students and recognizes that technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work and life.

This Acceptable Use Policy (AUP) defines the guidelines and behaviors that students and employees and guests are expected to follow when using school technology resources. The use of technology exacts certain responsibilities on the parts of employees, parents and students and is provided as a privilege, not a right. This AUP is a promise that the responsibilities inherent to technology use will be respected.

Technologies Covered

HCS D may provide Internet access, desktop computers, laptop computers or other mobile devices, videoconferencing and online collaboration tools, message boards, email, and more. As new technologies emerge, HCS D will attempt to provide access to these tools if appropriate. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for educational purposes. All students and employees are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be respectful, responsible, safe, and ready to learn; not try to get around technological protection measures and use good common sense.

Internet Access

HCS D provides its students and employees with access to the Internet, including web sites, resources, digital content, and other online tools. That access will be restricted in compliance with Child Internet Protection Act (CIPA) regulations and school policies. Web browsing is monitored and web activity records may be retained indefinitely.

Students and employees are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Internet. If a site is blocked and a student or staff believes it should not be, the user should follow district protocol.

Digital Citizenship

Students and staff should always use the Internet, network resources, and online sites in a courteous and respectful manner. Students and employees should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet *unless it is required to perform their job or educational duties*. Students should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it is there permanently – and can sometimes be shared and spread in ways you never intended.

Remote Learning

During remote learning, students shall be held to the same standards set forth in the Code of Conduct, including the prohibited conduct and potential penalties. Remote learning sessions and

content must not be recorded in any way without permission, including, but not limited to, taking videos, photos or screenshots. Remote learning sessions and content must not be shared on any social media platform or other similar means. Students may not display any virtual backgrounds, photographs or objects during a videoconference or during remote learning that would violate the Code of Conduct. Students should ensure that there is nothing in the background during their meeting that would be against school policy to have in the classroom. During remote or hybrid learning, all users are expected to adhere to the same behavior, academic integrity and acceptable use standards as for in-person learning. Only district-approved systems and platforms may be used for remote learning

Email

HCS D may provide students and employees with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If students or staff are provided with email accounts, they should be used with care. Students should not send personal information *unless required for an assignment*; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher. Students and employees are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/ Collaborative Content

Recognizing the benefits collaboration brings to education, HCS D may provide students and employees with access to web sites or tools that allow communication, collaboration, sharing, and messaging for educational purposes. Students and employees are expected to communicate with the same appropriate safe, mindful, courteous conduct online as offline. Use of such sites or tools on the district's network and/or using district devices may only be for school purposes. Posts, chats, sharing, and messaging may be monitored. Communicating over the Internet brings anonymity and associated risks, and employees and students should carefully safeguard the personal information of themselves and others. If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home or supervisor in the case of an employee) immediately. Students should never agree to meet someone they meet online in real life.

Security

Students and employees are expected to take reasonable safeguards against the transmission of security threats over the school network including the wireless 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 computer or any mobile or any removable device you are using might be infected with a virus, immediately turn off the device and please alert the IT helpdesk. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Students and employees should not download or attempt to download or run .exe programs over the school network or on school resources without express permission from IT helpdesk. 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 education purposes. Students and staff should not download files to external drives via the network or wireless files sharing, nor should they utilize programs installed on external media such as flash drives, or CDs, as a way to work

around installing a program on their device(s).

Laptop, Tablet and Removable Devices Policy

HCSD may provide students and employees with laptop or tablet computers or other removable devices to promote learning outside of the classroom. Students and employees should abide by the same Acceptable Use Policy when using school devices off the school network as on the school network. Students and employees and guests are expected to treat district owned devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Students and employees should report any loss, damage, or malfunction to IT staff immediately. Students and employees may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

Personally-Owned Devices Policy

Employees should keep personally-owned devices (including laptops, tablets, and Chromebooks) turned off and put away during school hours – unless in the event of an emergency or as instructed by supervisor for educational purposes. Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from IT staff. In some cases, a separate network may be provided for personally-owned devices.

Students are discouraged from bringing any personal internet-enabled devices to school during the school day. Primary school students must silence any device brought to school and keep it in the classroom teacher's storage container, the student's personal cubby or locker. Middle and high school level students must keep any such devices silenced and stored in student lockers.

Plagiarism

Students should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Students should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online or in another source. As with any research, sources should be appropriately cited, giving credit to the original author. No student should submit work created by or in part directly from an AI tool, unless specifically approved by the teacher.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Do not be mean. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Artificial Intelligence

Hudson City School District encourages the thoughtful use of district-approved AI tools to enrich teaching, learning, and daily operations. Students and staff may employ AI for research, creativity, and productivity so long as they (1) protect privacy and comply with Education Law 2-d, (2) cite or verify any AI-generated content, and (3) follow all academic-honesty and acceptable-use rules. Entering sensitive data, relying on unapproved platforms, or submitting undisclosed AI-produced work is prohibited.

Student PII should not be disclosed to an AI source without prior express written permission from

the district's Data Protection Officer. Staff must be mindful that some AI tools are free and others are not, that some AI tools are not permitted to be used by individuals under certain ages, and that some AI tools require parent permission. All users need to recognize AI tools may produce false answers or information, or information that is stale, and therefore responses and content must always be carefully verified before used for district, professional or educational purposes through a reliable source such as textbooks, scientific papers, and/or reputable educational resources. Citing any AI source as a primary source of information is not permitted.

Computer/Network Acceptable Use for Students

HCS D shall not be liable for inappropriate use of electronic computer and/or communications resources, violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users for any reason.

HCS D shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet, network, or any other form of computer use and/or electronic communication.

Access to HCS D's computer network and/or electronic communications systems is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of the following regulations governing the use of the systems and shall agree in writing their compliance with such regulations. Non-compliance may result in suspension of access or termination of privileges or other disciplinary action. Misuse, theft or vandalism of HCS D computer network and/or electronic communications systems in any way will not be tolerated.

Examples of Unacceptable Use

I will not:

- Use school technologies in a way that could be personally or physically harmful.
- Share my personal log-in/password with others.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally-identifying information about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that is not intended for my use.
- Create, share, distribute or sell sexually explicit or other inappropriate materials

This is not intended to be an exhaustive list. If you are unsure whether or not a particular action is acceptable, please bring it to the attention of an adult

Violations of this Acceptable Use Policy

Violations of any of these rules may result in consequences, commensurate with the district Code of Conduct, including, but not limited to, loss of technology use privileges, as well as a failing grade or suspension in the case of students, and disciplinary charges in the case of teachers and staff.

Parent Permission Form/ Student Acceptable Use Policy Agreement

Please complete ALL SECTIONS and return this form to the school office.

By signing the permission form, the Hudson City School District, its employees and/or any affiliated institutions will be released from any and all claims of any nature that may result from a student's use of, or inability to use, our computers and network, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

Student's Name _____

Grade: _____

School: _____

Teacher _____

Please circle YES or NO

My child has access to the Internet at home for their schoolwork **YES NO**

Student Use Agreement

As a Hudson City School District Student, I have reviewed the **Computer / Network Acceptable Use Policy (AUP)** with my parents and I agree to comply with these rules.

Student Name (Please Print) _____

Student Signature _____ Date _____

Parent Permission for Student Technology Use

As a parent or guardian of a student at Hudson City School District, I have read the **Computer / Network Acceptable Use Policy (AUP)** and I understand this agreement will be kept on file at my child's school. (Questions should be directed to the principal for clarification.)

My child may use the computer/instructional network according to the rules outlined in the AUP.

YES NO

My child may use the Internet according to the rules outlined in the AUP.

YES NO

Parent Name (Please Print) _____

Parent Signature: _____

Employee Acceptable Use Policy (AUP) Agreement

The Hudson City School District (HCSD) computer network and electronic communications system shall be made available to students and employees for instructional, research, and administrative purposes exclusively.

Electronic mail use or other use of the electronic communications and computer systems by employees is not considered private. Designated staff shall be authorized to monitor such computer use and/or electronic communication at any time to ensure appropriate usage as set forth in this document.

HCSD shall not be liable for inappropriate use of electronic computer and/or communications resources, violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users for any reason.

HCSD shall not be responsible for ensuring the accuracy or usability of any information found on the Internet, network, or any other form of computer use and/or electronic communication.

Access to HCSD's computer network and/or electronic communications systems is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of the following regulations governing the use of the systems and shall agree in writing their compliance with such regulations. Non-compliance may result in suspension of access or termination of privileges or other disciplinary action. Misuse, theft or vandalism of HCSD computer network and/or electronic communications systems in any way will not be tolerated.

Violations of the AUP Agreement may result in criminal prosecution as well as disciplinary action. Prohibited uses include, but are not limited to: *

- Copying, installing, or storing non-approved software or files without specific permission.
- Accessing another user's account or password without official authorization.
- Use of confidential or personal information without consent of HCSD.
- Use for non-school district related commercial or business purposes, including advertising.
- Obscuring the true identity of user logging in and/or sender of electronic mail.
- Accessing or intentionally destroying files or software without permission.
- Any attempt at bypassing network or internet security devices or programs.
- Inhibiting or interfering with the use of the HCSD communications network.
- Transmitting information containing obscene, indecent, or disrespectful material.
- Violating any laws or participating in any crime.
- Using the computer to harass others, including unacceptable language, images, or threats.
- Tampering, theft, or vandalism in any form of computers, networks, printers, scanners, cameras, or associated equipment in any way.

**This is not intended to be an exhaustive list. If you are unsure whether or not a particular action is acceptable, please bring it to the attention of a supervisor.*

I have read, understand, and agree to abide by the provisions of the Employee Acceptable Use Policy of the Hudson City School District.

School: _____ Position: _____

Name: _____

Signature: _____

Date: _____

Please return this form to the Central Office where it will be kept on file. It is required for all staff that will be using the computer network, email system, and/or Internet access.

Revised: March 27, 2017
Updated & Re-Adopted: September 3, 2019
Updated & Re-Adopted: June 15, 2021
Updated & Re-Adopted: December 15, 2025