HUDSON CITY SCHOOL DISTRICT

Claverack · Ghent · Greenport · Hudson · Livingston · Stockport · Taghkanic

Mobile Device Equipment Loan Form

For the 2024-2025 school year, Hudson City School District students will be loaned district mobile device equipment (Chromebook, iPad, hotspot, etc.) based on their grade level and program. These devices are to exclusively be used as a learning tool within, and outside of, school hours. While the district has agreed to loan this device to your student, it is essential that the following guidelines be followed to ensure the safe, efficient and ethical operation of this loaned device(s). Please refer to Policy 5300 Student Code of Conduct – Section 5300.30 Prohibited Student Conduct, Letter A, #7, Letter D, #6, and Letter I on pages 15-18. ***(Please review and sign both sides of the document.)***

- I will supervise my child's use of the device(s) at home.
- I will discuss my expectations regarding the use of the Internet at home.
- I will supervise my child's use of the Internet.
- I will not attempt to repair the Chromebook, nor will I attempt to clean it with anything other than a soft, dry cloth.
- I will not load or delete any software from the Chromebook.
- I agree to return the device to school when requested and/or upon my student's withdrawal, transfer or graduation from the Hudson City School District.
- I understand and agree that this equipment is, and at all times remains, the property of Hudson City School District and is loaned to my student for educational purposes. The device does have identification on it indicating that it is the property of HCSD and that identification **should not be altered, removed or modified** in any way. These devices are assigned and registered to each student individually, similar to a textbook or sports jersey and I am responsible to return the device and charger at the time and date indicated by the school.
- I understand that while normal wear and tear is expected, the device needs to be returned in working condition with no cracks, missing parts, broken parts, etc. I understand that if the device is purposefully damaged, lost or stolen and not covered under warranty, I am responsible for the cost of the repair or replacement as with all other district-owned property provided to my student for educational purposes (jerseys, library books, etc.).

2024-2025 Replacement Costs:

iPad $250	iPad charger $20
CTL Chromebook $399 Dell Chromebook $250	Chromebook Charger $20
Chromebook Keyboard $17.95	Chromebook Front Cover $24.95
Chromebook Back Cover $18.95	Hotspot $40
Hotspot Charger $20	Hotspot Case $10
Chromebook Case $25	Chromebook Screen $100

- I understand and agree that stickers and/or tape should not be used on the device nor the case. **I understand that writing, drawing or painting on the device and case is considered vandalism.** Replacement costs and disciplinary actions may apply if stickers, tape, writing, drawing or paint cannot be removed.

24-25 Mobile Device Equipment Loan Form
Signature Page

- I understand that the primary purpose of the device is educational. To comply with federal regulations (CIPA and COPPA), policies and restrictions have been configured on the device to manage and monitor the device. Inclusive in these are web security filters on the device that will not allow students to access non-academic websites including social media.
- I agree to comply with HCSD BOE Policy #4526-E (Computer Network Acceptable Use Policy) regarding appropriate use of district computer resources and further agree to all parental responsibilities listed within this document,
- I understand it is **mandatory that the Chromebook remains in the district-provided case**.

I have read, understand, and agree to abide by the provisions in the 2024-2025 Mobile Device Equipment Loan form for borrowing a district issued Mobile Device and/or hotspot.

Student Name: _____ Grade: _____
Student Signature: _____
Parent's Name: _____
Parent's Signature: _____
Date: _____

For Office Use Only

Chromebook	Hotspot
Chromebook Serial/Service Tag: _____	Hotspot Name/Number: _____
Chromebook Asset Tag: _____	Hotspot IMEI: _____
Charger #: _____	Hotspot Asset Tag: _____

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**

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.)

1. **My child may use the computer/instructional network according to the rules outlined in the AUP.** **YES** **NO**

2. **My child may use the Internet according to the rules outlined in the AUP.** **YES** **NO**

Parent Name (Please Print) _____

Parent Signature:_____ _____ Date: _____

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 _____

COMPUTER USE IN INSTRUCTION

The Board of Education is committed to optimizing student learning and teaching. The Board considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in and out of district classrooms solely for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

All users of the district's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility, as outlined in 4526-E, Computer/Network Acceptable Use Policy form.

The Board of Education has established regulations governing the use and security of the district's computer network. All users of the district's computer network and equipment shall comply with this policy and those regulations. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent shall be responsible for designating the Instructional Technology Manager to oversee the use of district computer resources. The Instructional Technology Manager, in conjunction with the Assistant Superintendent for School Improvement, will prepare in-service programs for the training and development of district staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent, working in conjunction with the designated purchasing agent for the district, the Instructional Technology Manager, Assistant Superintendent for School Improvement, and the Building Principals, will be responsible for the purchase and distribution of computer software and hardware throughout district schools. They shall prepare and submit, for the Board's approval, a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

Note: Policy added

Adoption date: July 9, 2007
Revision date: March 27, 2017
Revision date: June 15, 2021

COMPUTER USE IN INSTRUCTION
REGULATION

The following rules and regulations govern the use of the district's computer network system and access to the Internet by students and staff.

I. *Administration*

- The Superintendent of Schools will designate an Instructional Technology Manager to oversee the district's computer network.
- The Instructional Technology Manager will monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Instructional Technology Manager will be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The Instructional Technology Manager, in conjunction with Assistant Superintendent, will provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- The Instructional Technology Manager will ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- All student agreements and parental consent forms will be maintained by each building administrator or designee to abide by district policy and regulations
- All staff agreements will be kept on file in the district office to abide by district policy and regulations and forms.

II. *Internet Access*

- The Hudson City School District will make all reasonable attempts to provide Internet access for educational purposes.
- Students will be provided with an individual e-mail account and must only use their district provided email address.

Unless authorized by the District, the following will be prohibited:

- All users will be prohibited from using the Internet for personal use, including, but not limited to, accessing social networking sites; playing online games; purchasing or selling anything online; accessing personal email services; and watching videos online not related to class assignments.
- Students may not participate in unsupervised online chats not related to instruction.
- Students are not permitted to participate in Google hangouts.
- Students may not construct their own web pages or blogs using district computer resources unless authorized by a teacher as part of the curriculum.

Instructional staff members will be required to monitor all of these activities **to the extent possible.**

III. *Acceptable Use and Conduct*

- Access to the district's computer network is provided solely for educational purposes and research consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual, in whose name an access account is issued, is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords will be changed in accordance with the District's password protocol.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive, vulgar or intimidating language are all inappropriate.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or Manager of Instructional Technology and IT Helpdesk. Under no circumstance should the user forward or share the problem with anyone other than a district official or unless authorized by a district administrator.
- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

IV. *Prohibited Activity and Uses*

The following is a list of prohibited activities concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or another appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit or make available to others obscene, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are discriminatory, racist, sexist, abusive, threatening or harassing to others.
- Accessing another user's account or password without official authorization.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive email.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of another person unless a function of your job duties.

- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems. Installing personal software or using personal disks on the district' s computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Wastefully using consumable district resources
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other employees and generally accepted network etiquette.

V. *No Privacy Guarantee*

Students and Employees using the district's computer network should not expect, nor does the district guarantee privacy for electronic mail (e-mail) or any use of the district's computer network, even if an email is labeled "confidential" or "private". The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

VI. *Sanctions*

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secrets. Users must respect all intellectual and property rights and laws.

VII. *District Responsibilities*

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The district also

will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: July 9, 2007
Revision date: June 15, 2021

Computer/Network Acceptable Use Policy

The Hudson City School District (HCSD) 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 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
HCSD may provide Internet access, desktop computers, mobile computers or other mobile devices, videoconferencing and online collaboration tools, message boards, email, and more. As new technologies emerge, HCSD will attempt to provide access to these tools. 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.

Web Access
HCSD 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 Web. If a site is blocked and a student or staff believes it shouldn't 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's out there – 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 will not be recorded in any way without permission, including, but not limited to, taking videos, photos or screenshots. Remote learning sessions and content will 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.

Email
HCSD 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/Web 2.0/Collaborative Content
Recognizing the benefits collaboration brings to education, HCSD may provide students and employees with access to web sites or tools that allow communication, collaboration, sharing, and messaging among others. Students and employees are expected to communicate with the same appropriate safe, mindful, courteous conduct online as offline. 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.

Mobile Or Removable Devices Policy
HCSD may provide students and employees with mobile 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 are expected to treat these 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
Students and 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 a teacher or 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.

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 didn't create themselves, or misrepresent themselves as an author or creator of something found online or in another source. As with any research v should be appropriately cited, giving credit to the original author.

Cyber bullying
Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Don't be mean. Don't 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, cyber bullying can be a crime. Remember that your activities are monitored and retained.

Computer/Network Acceptable Use for Students

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, 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 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.

Examples of Acceptable Use
I will:

- Use school technologies for school-related activities.
- Keep my personal log in/password to myself.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

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.

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 isn't 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, including, but not limited to, loss of technology use privileges, a failing grade, suspension, expulsion, financial liability and/or legal action.

Dr. Juliette Pennyman, Superintendent of Schools

Student Digital Resources Survey

2024-2025 School Year

Please note that your student will be issued a device by Hudson City School District

Student Information	
First Name:	
Last Name:	
Date of Birth:	
Grade:	

Device Information

What is the device your child uses most often to complete learning activities away from school? (This can be a school-provided device or another device, whichever the student is most often using to complete their schoolwork.)

- ☐ Desktop
- ☐ Laptop
- ☐ Tablet
- ☐ Chromebook
- ☐ None

Who is the provider of the primary learning device?

- ☐ Personal
- ☐ School

Is the primary learning device shared with another student in the household?

- ☐ Shared
- ☐ Not Shared

TURN OVER TO COMPLETE PAGE 2

Is the primary learning device sufficient for your student to fully participate in all learning activities away from school?

- ☐ Yes
- ☐ No

Internet Access Information

Is your student able to access the internet in their primary place of residence?

- ☐ Yes
- ☐ No

What, if any, is the primary barrier to having sufficient and reliable internet access in your student's primary place of residence?

- ☐ Availability
- ☐ Cost
- ☐ None
- ☐ Other: _____

What is the primary type of internet service used in your student's primary place of residence?

- ☐ Residential Broadband
- ☐ Cellular
- ☐ Mobile Hotspot
- ☐ Community WiFi
- ☐ Satellite
- ☐ DSL
- ☐ None
- ☐ Other: _____

In their primary residence, can your student complete the full range of learning activities, including video streaming and assignment upload, without interruptions caused by slow or poor internet performance?

- ☐ Yes
- ☐ No