BOARD OF EDUCATION
Cherry Hill, New Jersey

POLICY 6142.12

ACCEPTABLE USE OF TECHNOLOGY

Introduction

The Board of Education encourages the use of technology in the classroom as an educational tool and to promote student achievement. To achieve this, the Cherry Hill School District strives to maintain an array of technology and telecommunication equipment, which is made available to all students and staff members. In an effort to maintain high standards of technology, the following policies have been put into place to ensure the safety and security of the district network, as well as the safety and security of those who are using it.

Technology, as defined in this policy, refers to any software, computer hardware, [video conferencing] equipment, or device owned by the District or student/staff member that makes a connection to the Cherry Hill Public Schools (CHPS) network.

The Internet connectivity and other network resources that are provided by the Board of Education are for the purpose of allowing students and staff to access unique resources, to support research, and to promote collaboration.

What constitutes acceptable use?

The Board of Education for the Cherry Hill Public Schools supports the use of the Technology and the Internet in the district's instructional program. "Acceptable use" is defined as any educational activity involving technology that is approved by the teacher in a classroom setting, including research and collaboration. Students are allowed to utilize school and personal devices in conjunction with the district network to retrieve information and run specific software applications as directed by their teachers for enhancing the classroom learning experience. For instructional purposes, the use of technology and the district network shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities and developmental levels of the students.

Outside of a classroom setting, Acceptable use, including use of staff and student personal devices is defined by the guidelines outlined below.

Computer / Internet is a privilege

Use of the Internet is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules may result in cancellation of the privilege. The Board of Education, under this agreement, is delegated the authority to determine appropriate use and may deny, revoke, suspend or deny access to any user account at any time based upon its determination of inappropriate use by an account holder or user.

Liability Disclaimer / No Warranties

The District makes no warranties of any kind, express or implied, that the functions or the services provided by or through the CHPS network will be error-free or without defect. The District will not be responsible for any damage users may suffer including, but not limited to, loss of data or interruption of service. The District is not responsible for financial obligations arising through the unauthorized use of the CHPS network.

Filtering

The District is in compliance with the Children's Internet Protection act and uses technology protection measures that block and/or filter visual depictions that are obscene as defined in section 1460 of Title 18, United States Code; child pornography, as defined in section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphics image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual, acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

When an Internet site with legitimate educational value is inadvertently blocked, a district technology staff member may override the protection measures that blocked and/or filtered that site upon receiving a written request from a district staff member.

Illegal/ Prohibited Activities

Use of CHPS network for any illegal activities that violate federal, state, or local laws and regulations is prohibited. Illegal activities include, but are not limited to:

- Accessing or distributing material that is obscene, pornographic, harmful to minors or otherwise inappropriate for educational use.
- Downloading or storing movies, music, software, games, documents or other materials on the district network which would violate copyrights or licensing agreements. Students' folders are subject to inspection by members of the technology department, and files that violate this policy will be deleted without notice.
- Accessing any district system or file without authorization, stealing data or other intellectual property, invading the privacy of others, vandalizing data of another user, intentionally disrupting network traffic.
- Tampering with district equipment or computers to crash, degrade, disrupt or bypass the district network.
- The use of proxies, remote software or any other means to bypass the district web filter.
- Utilizing the district computer network to operate a business, or to publish/host a website unless authorized by a staff member for educational purposes.

Monitoring of equipment

Technology equipment and the CHPS network is property of the District, and all computer software and hardware belong to it. Therefore, the District retains the right to monitor all access

to and use of the Internet, e-mail, computers and the district network. The system is designed to keep a record of all activity on and off the Internet, and this information is also district property. It is important for all users to understand that no use of the Internet or e-mail can ever be guaranteed private.

School building staff and/or faculty will have the ability to monitor students' use of the Internet, through either direct supervision, or by monitoring Internet use history, to ensure enforcement of this policy.

Security / Safety

a. Password security

Staff and students entering the CHPS are issued a network login and password for their exclusive use. The combination of a user login and password is not to be shared with anyone at any time. Logins and passwords are in place to protect information contained in district network resources. User names and passwords will be used to log into the wireless CHPS network on personal devices as well as district owned devices.

b. Private information

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender. Users shall not publish private information about another individual.

The district respects and values privacy. In order to maintain system integrity and to ensure responsible use of district technology however, the district technology department has the capability to view the contents of any file server, workstation, laptop or district email. Therefore, users of CHPS equipment, network, or website should have no expectation of privacy regarding their use of district property, network and/or Internet access.

c. Information Security

Students should only use electronic mail, chat rooms, social media and other forms of direct electronic communication for school related purposes as directed by staff, and will not disclose personal information such as name, school, address, and telephone number to others outside of the district network except under the direct supervision of a staff member

d. Staff Communication with students

Electronic communication with students shall be conducted only via district online facilities and systems or outside/public systems or services explicitly approved by the administration of the district.

Personally Owned Electronic Devices

A Personal Electronic Device is described as any electronic device that would have the capability to connect wirelessly to a network. Cherry Hill Public Schools offers filtered wifi access in each building. Students and Staff are permitted and encouraged to use personally owned electronic devices as educational tools within the classroom to expand the access to

knowledge and enable the communication between students, staff, parents and the world around us.

- Staff and students utilizing personal devices while on district property, do so at their own risk. The District assumes no responsibly for personal devices that are stolen, damaged or lost.
- Staff and students are advised to take reasonable precautions to prevent damage to or theft of personal devices. Staff members are not to secure student personal devices for their students, as it is the student's responsibility for their own device.
- Functionality including but not limited to: wifi set-up/connection, maintenance/updating, charging, software and operation of the personal electronic device, is solely the device owner's responsibility. Charging facilities may not be available or provided at school, students should plan to bring personal devices to school fully charged.
- The District Technology Department will confirm that the district wifi network is working correctly within the building, but will not provide technical support for personal electronic devices.
- Personal devices may have the ability to connect to cellular networks and enable features beyond what is available on the district wireless network. (i.e. Text Messaging) Use of any of these features may involve costs or charges that are not within the control of the District and will be the responsibility of the owner of the device. Should a device connect to a network other than the district's, the device may have access to content not suitable for school, and the user of the device is still expected to abide by district acceptable use guidelines while the device is in use on school property.
- Using personal devices is a privilege and may be revoked at any time. Staff and students are permitted to use personal devices per the posted "zone" within their school.
    a. Green – Full access to personal devices is permitted
    b. Red – Access to personal devices is prohibited

Violations of this Acceptable Use Policy

Individuals violating this policy shall be subject to the consequences as indicated below and other appropriate discipline which is listed in the district code of conduct, including but [is] not limited to:

- Use of the network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Revocation of computer privileges
- Suspension from school
- Expulsion from school; and/or
- Legal action and prosecution by the authorities

Signature for AUP / Consent

No student shall be allowed to use the CHPS network and the district Internet connection unless a consent form signed by the student and his/her parent(s)/guardian(s) is on file at the schools which the student attends.

No staff member shall be allowed to use the CHPS network and/or the district Internet connection unless a signed consent form is on file with the District.

Legal References:
N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act

Adopted: 8/28/01
Revised: 8/28/07, 11/25/08, 3/27/12, 6/25/13