CROTON-HARMON SCHOOL DISTRICT

4526-R ACCEPTABLE USE FOR COMPUTER AND INTERNET ACCESS REGULATION

Use of the District's computers, electronic/digital devices and Internet use is a privilege. It serves as a point of voluntary access to information and ideas and as a learning laboratory for students as they acquire critical thinking and problem solving skills. Inappropriate use of the district's computer resources and electronic/digital devices is not only a policy violation, but may result in cancellation or suspension of those privileges at the discretion of a student's building principal or a staff member's administrator. The appropriate administrator will determine whether a policy violation has occurred, and the appropriate sanction. A policy violation may result in suspension or revocation of computer and Internet privileges, even for a single violation.

Every District student, staff or community member using the District's computers, electronic/digital devices and/or the Internet must acknowledge his or her acceptance of the attached Acceptable Use Contract for Computer and Internet Use before access to the District's computers and the Internet will be granted.

The District Technology Coordinator shall develop and implement procedures to monitor and enforce compliance with this regulation.

A copy of this Regulation shall be available in the main office of each school, and shall be posted in the computer laboratory.

***Terms and Conditions*:**

1. Acceptable Use: The use of the district's computers and/or electronic/digital devices or the maintenance of an account on the district's network by a student must be in support of education and research and consistent with the educational objectives of the District. Use by teachers and other staff members of the district's network or computing resources must comply with the rules appropriate for that network.

Recognizing that no list of sanctioned behaviors is completely exhaustive, these prohibited behaviors include, but are not limited to:

- Using profane, abusive or obscene language in either private or public messages
- Placing information obtained or used unlawfully on the Internet
- Using the Internet illegally in ways which violate federal, state and local laws
- Sending information over the Internet that is likely to damage the recipient's work or system
- Using the Internet for commercial purposes--specifically, offering or providing products or services
- Posting or e-mailing unauthorized solicitations on behalf of charities, other organizations or persons
- Using the Internet for more than incidental personal use
- Sending or knowingly receiving copyrighted material without permission
- Using another person's log-in credentials
- Using the Internet for accessing, sending, or receiving pornographic materials, similar inappropriate text files, or files dangerous to the system
- Circumventing security measures on school computers or computers outside the school network
- Falsifying one's identity to others while using the Internet
- Posting or sending private student or District employee information, or any other information that might result in a violation of privacy
- Downloading unauthorized software from the Internet
- Downloading audio or video files not related to appropriate academic, administrative or co-curricular activities
- Unauthorized distribution of copyrighted, trademarked or patented materials
- Installing unauthorized software programs
- Changing any computer files that do not belong to the user
- Attempting to gain access to files which are not publicly available

- Attempting to access sites on the Internet that are known to contain material inappropriate for schoolwork
- Using the Internet to harass or harm other people
- Sending hate mail, making discriminatory remarks, and any other similar antisocial activities
- Engaging in use with the purpose to cause others personal humiliation or embarrassment

2. Privileges: The use of the Internet/Computer Network is a privilege, not a right, and inappropriate use will result in cancellation of that privilege by the Superintendent or his/her designee. Any problems and/or questions must be directed to the Superintendent or such designee. The Superintendent, administration, faculty and staff of the District may deny, revoke, or suspend specific user accounts at their discretion for any misuse or violation of this policy. If the student's privileges have been revoked and the student has an assignment which requires use of the Internet, the teacher will give a comparable assignment not requiring use of the Internet. If this is not possible, then the Internet research can only be done, at the school, with adult supervision at all times. Individuals have the full responsibility for the use of their accounts, and a user of the district's computers or network must not share his or her account or password with any other person. Any sharing of passwords or the use of accounts of other persons is prohibited. All recipients of accounts must participate in training pertaining to the proper use of the network. Account users are responsible for maintenance of their accounts. The Superintendent or his or her designee will conduct a review of all accounts to determine adherence to this policy.

3. Netiquette: Individuals are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

a. Be polite. Do not be abusive in your messages to others.

b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.

c. Do not reveal your personal address, phone number, social security number, or credit card number, or such information for other students or colleagues.

d. Note that electronic mail (e-mail) and data files are not guaranteed to be private. People who operate the system have access to all mail and data. Message or other electronic data relating to or in support of illegal activities may be reported to the authorities or the Superintendent or his/her designee.

e. Do not use the network in such a way that will disrupt its use by others.

f. All communications and information accessible via the network should be assumed to be the property of the provider.

g. Use of the system and the data acquired must be in strict compliance with the law.

4. Disclaimer: The District makes no warranties of any kind, whether expressed or implied, for the service access or information it is providing pursuant to this policy. The District will not be responsible for any damage suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the District's negligence or error or omissions. Use of any information obtained is at the user's risk. Any violation of State, of Federal or local laws, ordinances, rules, or regulations, and any attended penalties, shall be the sole responsibility of the individual(s) who abuse the system, violate this policy and/or the law. The District specifically denies responsibility for the accuracy or quality of information obtained through Internet services. It is the responsibility of each user to verify the integrity and authenticity of the information that is used.

5. Commercial Services: Commercial services are available on the Internet. If a user chooses to access these services, the user is liable for any costs that may be incurred.

6. Security Issues: If any user identifies a security problem on the Internet/Computer Network, they must notify the Superintendent or his/her designee. Any unauthorized attempt to login to the Internet/ Computer Network purporting to act as a system administrator will result in cancellation of user privileges. Any user identified as a

security risk or having a history or problems with other computer systems may be denied access to the Internet/Computer Network.

7. Vandalism: Vandalism will result in cancellation of privileges. Vandalism includes any malicious attempt to harm or destroy District equipment, software or data, or that of another user, the Internet or any agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses. In the case of vandalism to District equipment, the user will be financially responsible to reimburse the District for repair or replacement of said equipment.

8. District Right to Access Users' Computers and Accounts: Communication through the Internet or the District's networks is not considered private and there should be no expectation of privacy regarding any computer use of school district computers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Network administrators may remove or delete files, material and/or communications that are violative of district policy.

9. Use of Online Services from Internet Educational Resource Providers: As part of the district's instructional program, students (and their parents/guardians) and staff may be provided with access to and use of accounts from an outside internet educational resource provider, such as Google, through which access will be provided to that provider's services. The district shall comply with all contractual and other requirements related to the use of such services by its students (and their parents/guardians) and staff, and shall ensure that all such users execute any consent or authorization forms required for such use.

10. Use of Online Services for Learning: Teachers or other staff recommending or assigning the use of online services by students must verify in advance that the service is listed on the district's Approved Services List, or must obtain pre-approval by the Technology Coordinator, to ensure that adequate measures are in place to maintain student safety and privacy, in accordance with Policy 8630, Computer Resources and Data Management.

Ref:

Cross-ref:

- 4526, Access to Computer Network for Use In Instruction
- 4526-E, Acceptable Use Contract for Computer and Internet Use
- 4526.1, Internet Safety
- 4526.1-R, Internet Safety Regulation
- 8630, Computer Resources and Data Management
- 8635, Information Security Breach and Notification
- 8635-R, Information Security Breach and Notification Regulation
- 8650, School District Compliance with Copyright Law
- 8650-R, School District Compliance with Copyright Law Regulation

Adoption date: March 12, 2015

Revised: June 15, 2017

Croton-Harmon Schools