First reading: 2/4/14
Second reading: 5/20/14
Adopted by the School Committee: 5/20/14
First revised reading: 8/11/2020
Second revised reading: 9/01/2020
Adopted by the School Committee: 9/01/2020

10110: Responsible and Acceptable Use of District Technology Systems

Technology

1. Introduction

The East Greenwich School District (the "District") is committed to the smart use of technology to support our vision of a graduate who is knowledgeable, connected, reflective, and competent. These technologies, when properly used, promote educational excellence by connecting our students with the world-at-large and encouraging the effective use of technology by facilitating resource sharing, innovation, and communication.

The District provides our education community (staff and students) technology systems, network resources, and access to the information and tools available on the Internet. This access is granted solely for educational purposes and the administrative and business operations of the school district; however, the District acknowledges that students and staff may use District technology for incidental personal use.

This Responsible & Acceptable Use Policy ("RAUP") sets forth expectations for responsible and acceptable use by staff and students of District technology, including District-owned or leased digital devices, network resources, and Internet services for educational programs, as well as the administrative and business operations of the District.

As used in this policy, "user" includes anyone using computers, Internet, email, chat rooms, and all other forms of electronic communication or equipment provided by the District regardless of the physical location of the equipment or user. The RAUP applies even when District-owned equipment (laptops, tablets, etc.) is used off of District property.

2. District Responsibility for Providing a Safe Technology Environment

The District has a responsibility to provide a safe technology environment for its educational community, in compliance with federal and state law. To do so, the District will employ internet filtering, user monitoring, and other mechanisms set forth in District Policy #10210 Internet Safety.

3. Responsibilities and Opportunities for Students and Staff

The duty to educate students about responsible and appropriate use of the Internet and digital devices is shared by parents, teachers, and schools. It is the responsibility of students and parents to ensure that District-owned or leased digital devices, network, and internet services are used in accordance with these responsible use guidelines.

Staff and students will receive appropriate guidance and training toward best practices, good digital citizenship, and compliance with this RAUP and other District policies that govern the use of District technology systems and devices.

4. Online Educational Services

Students may be given assignments through online educational services, such as Google Apps for Education. Access to these sites is monitored by the District in order to provide a safe and secure learning environment for students. The District may create student email addresses, login credentials (e.g., usernames and passwords), and/or online profiles to allow students to access certain sites/services; however, these addresses, credentials, and profiles will only be used for the purpose of school assignments. A list of online educational services used in the educational process will be posted on the District's website.

5. Guidelines for appropriate and ethical use of District Internet and Network Services

The following guidelines provide a framework for the responsible, appropriate, and ethical use of District technology devices, tools, and services. Failure to comply with the guidelines set forth below may, at the discretion of the school and District administration, result in disciplinary action.

A) Users may access District devices, tools, network services, and Internet access for educational purposes only. The District may bar access to certain material which is not deemed educational or in support of District administration or business operations. Users are forbidden from circumventing security measures on school or remote computers and the District network.

B) Use of the District network system in a manner that encumbers system and network resources to the point that usage causes interference with others' access and/or services is prohibited.

C) Users shall always cooperate with requests from teachers and other school administrators for information about the users' computing activities.

D) Protection of users'personal information

i. Personal user accounts will not be used for instructional or educational purposes. Users will use a District-provided account for school/educational purposes and maintain the privacy and security of their usernames and passwords for all

network, Internet, social media, and online/cloud services (such as, but not limited to, Google Apps for Education).

ii. District-assigned user accounts inactive for three or more months (i.e. no logins or file uploads) will be deleted as they pose a security risk and tie up valuable system resources.

iii. Users shall not reveal their full name, home address or telephone number, or the personal information of others on the Internet without permission from a supervising teacher. Students are not to meet people they have contacted through the Internet without parental permission.

iv. Users are responsible for their account(s). Users should make appropriate use of the system and network-provided protection features and take precautions against others obtaining access to their computer resources, except that a parent or guardian may have access to their child(ren)'s District-issued log-on and password for educational uses. Individual password security is the responsibility of each user.

v. Users shall not use another user's account or password without proper authorization from their supervising teacher, other District administrator(s), or the system administrator.

vi. If a user believes that their user account and password has been compromised, they should immediately contact their teacher, supervisor, or school administrator.

6. Unauthorized Uses of the Internet or District Digital Devices

A) Obscenity and harassment

i. Users shall not use the Internet for illegal, unethical, or obscene purposes. Users are to inform their supervising teacher or supervisor if they access information or messages that are inappropriate or make them uncomfortable in any way. Use of the District network to post, send, or retrieve pornographic material, inappropriate text or graphic files, or files that could damage the network (i.e., files containing malware, worms, viruses) are prohibited.

ii. Users shall not harass other users by sending unsolicited, commercial, annoying, obscene, libelous, offensive or threatening messages (such as, but not limited to, email, social network postings, and direct messages), or use any form of electronic media to harass another person or group (i.e., cyberbullying). Users are to report any conduct they feel can be defined as harassment to a teacher, supervisor, or school administrator immediately.

iii. Sending or receiving unlawful information via electronic communications, using electronic communications illegal in ways that violate local, state, federal or international laws or statutes are prohibited.

B) Copyright laws and plagiarism

i. Users shall not plagiarize or download unauthorized copyrighted or licensed material. The District is not responsible or liable for materials in violation of copyright laws. Users are responsible for the content of their postings and obtaining all necessary permissions or licenses for any material used.

ii. Users shall not duplicate or distribute unauthorized copyrighted or licensed materials.

C) Downloading, accessing, or copying materials for non-educational purposes

i. Users shall not download or install any software, apps, movies, or games onto the digital devices, or change system configurations.
ii. Users shall not make copies of system configuration files for their own unauthorized personal use or to provide to other people/users.

D) The unauthorized collection of email addresses ("harvesting") from the Global Address List and other District directories is prohibited.

E) Commercial and political business

i. Users shall not use the Internet to access or disseminate "for profit" or commercial business material. No personal money-making activity may be conducted using District computing and networking resources.
ii. The District network and computing resources shall not be used for political lobbying or outside interests not related to District business.

F) Device and network security

i. Users shall not attempt to hack or otherwise breach security of any District-owned or leased digital devices, District servers, or any other user's account.
ii. Users shall not download, install or run security programs or utilities which reveal weaknesses in and/or bypass the security of a system.
iii. Users shall not attempt to circumvent or uninstall monitoring software from District-owned or leased devices. For example, users shall not run password cracking programs on any of District computer systems or install rootkits which bypass system security.

G) Use of the District network or a District digital device for any unlawful purpose is prohibited including, but not limited to:

i) Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, or copyrighted materials.
ii) Selling or purchasing illegal items or substances.

7. Consequences of violations

The District reserves the right to take immediate action regarding:

A) activities that create security and/or safety issues for the District, students, employees, schools, network or computer resources, or
B) activities in violation of CIPA and/or COPPA or

C) activities that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or
D) other activities as determined by the District as inappropriate.

If a user violates any part of these guidelines, consequences set forth all applicable federal and state laws, regulations, and District policies and protocols may apply, including, but not limited to provisions in District Policy #8310 Code of Conduct, and school student handbooks.

The District shall determine the appropriate disciplinary action for any prohibited student conduct. The District reserves the right without notice to freeze and delete an account that is engaging in activities that violate this RAUP or other District policies. The District reserves the right to disconnect any device that is the source of spamming, malicious or suspicious activities without notice until the machine in violation is cleaned or fixed.

8. Acceptance of the District's RAUP

Parents and legal guardians, with their child(ren), and should review the guidelines and sign a District-promulgated Technology Use Form, which should be returned to the child's school prior to issuance of a District-owned device, or, if a student does not borrow a device from the District, within 14 days of receipt of such Form.

By using the District devices, the network, and Internet access users have agreed to this policy. If a user is uncertain about whether a particular use is responsible or appropriate, he or she should consult a teacher, supervisor, or other appropriate District personnel.

9. Disclaimer

The District makes no warranties of any kind, whether expressed or implied, regarding the use of District-owned or leased digital devices, network resources, Internet access and use, or the accuracy, correctness, completeness, or reliability of any information, files, or software. The District shall not be responsible for damages for any of the foregoing, including loss of data, non-deliveries, or service interruptions, whether caused by its negligence, user errors or omissions, or other defects. Use of any information obtained via the Internet is at the user's own risk.

References:

Children's Internet Protection Act, 20 U.S.C. 9134, 47 U.S.C. 254
Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505
RI Gen. Laws § 16-21.6-1. Internet Filtering in Schools