First reading: 12/3/13
Second reading: 12/17/13, 1/28/14
Adopted by the School Committee: 1/28/14
First revised reading: 8/11/2020
Second revised reading: 9/01/2020
Adopted by the School Committee: 9/01/2020

10210: Internet Safety

Technology/Safety

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) 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 policy sets forth standards for meeting federal and state laws regarding safe access and use of the Internet as well as District expectations for staff and students.

The intent of this policy is to prevent (a) access to or transmission of inappropriate material via the Internet, Email, or other forms of electronic communication, (b) unauthorized access to any person's or organization's data by any means including "hacking" or "phishing" or any unlawful activity, (c) the unauthorized online disclosure, use, or dissemination of personal identification information of any student or staff in our out of the District, and (d) signify compliance with the Children's Internet Protection Act ("CIPA")

Internet Filtering

In accordance with CIPA, the District is required to have in place a filtering device on all computers with Internet access. The filter shall protect minors from access to visual depictions that are obscene or constitute child pornography, or that are harmful to minors, as outlined in CIPA.

The Internet access of all staff members are filtered with the same technology used to filter student access. The network provides educational resources for teaching and collaboration as well as business services for the operation of the school district. Staff may be granted greater access privileges to meet their specific position responsibilities; however, adherence to the same governing principles is expected of all users.

Misuse and Monitoring

The District shall implement and maintain network protection procedures to identify and prevent Internet misuse as defined in this policy by any network user. To "enforce" compliance with CIPA and Children's Online Privacy Protection Act of 1998 (COPPA) during the use of the District with Internet access, the District shall, as appropriate, review Internet filter logs and, in some cases, data on a device when there is reason to believe that the user is circumventing the Internet blocking or filtering technology. The District, therefore, reserves the right to access the data on a school-owned and school-loaned device to ensure that CIPA compliance is maintained.

It shall be the responsibility of all District staff to supervise and monitor Internet access in accordance with CIPA and COPPA. Further, it shall be the responsibility of all District users to report all suspected misuse of Internet access and use to the Director of Technology and/or the Assistance Superintendent of Schools.

Requests to Unblock Website

Websites that are blocked by the Internet filter may be unblocked based on the following criteria:

1. Educational purposes – Where access to the blocked site is consistent with the instructional needs of the grade level and or curriculum of the teacher requesting the site be unblocked as determined by the Director of Technology in collaboration with the Assistant Superintendent and where applicable the school principal.

2. Staff related purposes – A staff member needs a website unblocked related to their job (such as purchasing, law enforcement, bona fide research). Any person requesting to have a site unblocked should submit a formal request to the Director of Technology.

3. To unblock any blocked website the teacher or staff member requesting the site be unblocked must submit the request in writing by email to the Director of Technology.

4. If the request is deemed appropriate the website will be unblocked as soon as possible and the Director of Technology will immediately notify the requestor by email.

Denied Requests
If a request to unblock a website is denied, the Director of Technology will provide the specific reasons as to why the request was denied as well as the individual's right to appeal the decision. Further appeals may be made in writing to the Superintendent or the Superintendent's designee requesting that the denial be overturned.

Reporting
The Director of Technology will maintain a list of all requests for unblocking websites as well as the final determination of the request. Website unblocking request records will be public and available upon request.

In the event that there are significant requests for website filtering changes defined as ten or more in a single academic year, then the records will be used to review and consider modifications of current filtering policies and/or Internet filter changes.

Social Media and Blogs
The District recognizes social networking and social media websites can have an efficacious use in teaching and learning. Staff and students using such sites shall use the same governing principles as stated this policy as well as the requirements set forth in the District's Responsible Use (#10110) and Social Media (#10310) Policies.

Personally Identifiable Information
District Internet users shall at all times protect the personally identifiable information of all staff and students including but not limited to name, address, phone number(s), and email address. Additionally, staff shall not allow students, especially those under the age of 13, to access apps, social media sites, or blogs in an unsupervised manner that could compromise the protection of their personal information and safety. All such activities shall comply with the Children's Online Privacy Protection Act of 1998 ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA").

Enforcement and Modification
If a District Internet user including guest users are found to be misusing Internet resources and/or tools, the District reserves the right to limit and/or deny Internet access to maintain CIPA and COPPA compliance. In the event that a user misuses the Internet as defined in this policy reasonable and appropriate accommodations shall be put in place to maintain access for educational requirements or the administration or business operations

of the District, including but not limited to restricting device use and physical observation during Internet access. Procedures for disabling, modifying, or restricting Internet access in such situations shall be the responsibility of the Director of Technology and in collaboration with the Assistant Superintendent and school principal as appropriate.

Education and Training

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

Review and Update of Tools

The District will continuously review and evaluate the programs and procedures implemented to meet the requirements set forth in this policy, and reserves the right to update and change these measures, protections and trainings as the need arises.

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
Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
RI Gen. Laws § 16-21.6-1. Internet Filtering in Schools
Policy #10110 Responsible and Acceptable Use of District Technology Systems