SMYRNA SCHOOL DISTRICT
District Policy

Article: 6000 Instruction
Title: Computing and Internet Board Policy
Policy #: 6150

A. Purpose

1. The District provides employees and students with access to the district's wide area network (the Network), including Internet access and access to the district's email system.

2. The Network is focused on preparing students for success in life and work by providing electronic access to a wide range of information and the ability to communicate with people throughout the world. Additionally, the Network increases district intra-communication, enhances productivity, and assists employees in upgrading skills through exchange of information with peers. The Network enables the district to share information with the local community, including parents, social service agencies, government agencies, and businesses.

3. The Network shall not be used for commercial purposes (i.e. offering or providing goods or services or purchasing goods or services for personal use). District acquisition policies shall be followed for district purchase of goods or services through the Network.

4. The Network shall not be used for political lobbying. Employees and students in class activities may use the network to communicate with elected representatives and to express political opinions.

5. "Educational purpose" includes use of the network for classroom activities, off-site use, professional and career development.

B. District Responsibilities

1. The Superintendent or designee serves as the coordinator overseeing the Network and working with other state organizations, as necessary.

2. The Supervisor of Technology serves as the district level coordinator for the Network.

3. The Director of Curriculum ensures a broad selection of training activities are available, and ensures policies and handbooks regarding technology remain up to date and accessible.

4. The building principal approves building-level activities, ensures teachers receive proper training in the use of the Network and the requirements of this policy, establishes a process ensuring adequate supervision of students using the Network, and interprets the District Acceptable Use Policy at the building level.

5. The District Technology staff establishes a process for setting up individual and class accounts, sets quotas for disk usage on the Network, establishes a district virus protection process, maintains executed user agreements, and ensures compliance with district software licenses.

6. All instructional staff are responsible for educating~~,~~ and supervising, appropriate usage of the Network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

7. All staff are responsible for monitoring appropriate usage of the network and for reporting inappropriate usage.

C. Technical Services Provided through District Network

1. **E-mail** allows employees and students to communicate with people throughout the world and to engage in group discussions related to educational subjects. Staff are assigned accounts. Students have access to e-mail for educational purposes under the direct supervision of a staff member.

2. **The Internet** is a valuable research tool providing students and employees access to a wide range of information in the form of text, graphics, photographs, video, and sound.

3. **Remote Access** allows the user to log in to remote computers.

4. **Social Media** and class projects requiring participation in such activities will be conducted under the supervision of the staff member conducting the class.

5. **Filtering Software.** The state of Delaware through the Delaware Department of Technology and Information maintains software designed to block access to certain sites.
6. **Educational Applications** are used by the district to connect students to instructional content and up to date information to ensure student success.
7. **Classroom Monitoring Software.** Software provided by the state of Delaware through the Delaware Department of Technology and Information. Will be used to monitor, filter, detect and notify school staff of inappropriate and/or harmful content accessed or created by users. The classroom is anytime students are using a district program and/or device.

D. Access to the Network

1. Student use of the Network is governed by the Student Code of Conduct. Employee use is governed by employment contracts. The District's Acceptable Use Policy, set forth in Section L, outlines policies specific to computing and network use. All users are also governed by State network policies.

2. District employees and students will have access to the Internet through the district's networked computers. Parents may, however, request their child(ren) not be provided such access by notifying the district in writing.

3. **E-Mail-Students**. Individual E-mail Accounts for Students will be available for educational purposes.

4. **E-Mail-Employees.** Individual E-mail Accounts for employees will be provided with an individual account.

5. **Guest Accounts**. Guests may receive an individual account with approval of the Superintendent or designee if there is a district-related purpose requiring such access. Use of the network by a guest shall be limited to the district-related purpose.

E. Parental Notification and Responsibility

1. The district will notify parents about the Network/Digital Cloud Resources and the policies governing their use.

2. The District Acceptable Use Policy (see Section L) restricts access to inappropriate material. There is a wide range of material available on the Internet, some of which may conflict with the values of District families. It is impractical for the district to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes parents bear primary responsibility for transmitting family values to their children. The district will encourage parents to tell their child(ren) what material is and is not acceptable for their child(ren) to access through the Network.

3. The district will provide students and parents with guidelines for student safety while using the Internet, appropriate online behavior, and cyberbullying awareness and response.

F. District Limitation of Liability

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

G. Due Process

1. The district cooperates with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the Network.

2. Allegations a student violated the District Acceptable Use Policy are handled in ~~accord~~ accordance with the Student Code of Conduct.

3. Allegations an employee violated the District Acceptable Use Policy are handled in accordance with the employee contract.

4. The Superintendent or designee may terminate the account privileges of a guest user by providing notice to the user.

H. Search and Seizure

1. Network/Digital Cloud Resource users have no privacy expectation in the contents of their personal Network/Digital Cloud Resource files.

2. Routine maintenance and monitoring of the network/digital cloud resources may lead to discovery of user violations of the District Acceptable Use Policy, the Student Code of Conduct, employee contracts, or the law.

3. Searches will be conducted if there is a suspicion of a violation in regard to the District Acceptable Use Policy, the Student Code of Conduct, employee contracts, or the law.

I. Copyright and Plagiarism

1. District policies on copyright govern the use of material accessed through the Network. Because the extent of copyright protection of certain works found on the Internet can appear unclear, employees shall request permission from the holder of the work if use of the material has the potential of being considered an infringement. Teachers shall instruct students to respect copyright and to request permission when appropriate and to cite materials according to literary standards.

2. District policies on plagiarism govern use of material accessed through the Network. Teachers shall instruct students in appropriate research and citation practices.

J. Academic Freedom, Selection of Material, Student Rights to Free Speech.

1. Board Policy 5100, Student Rights and Responsibilities, governs the use of the Internet.

2. When using the Internet for class activities, teachers shall select material relevant to the course, and appropriate in light of the age of the students. Teachers shall preview the materials and sites required or recommended for student access to determine the appropriateness of the material contained on such sites. Teachers shall provide guidelines and lists of resources to assist students in focusing research, assist students in developing skills to ascertain the accuracy of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for divergent views.

K. District Web Site

1. The district shall establish a Web site and develop Web pages presenting information about the district. The Superintendent, or designee, shall establish a process for governance of the district's Web activities. At the discretion of the Superintendent, recognized district-wide organizations may also publish web pages on the district server.

2. Schools and classes may establish Web pages presenting information about the school or class activities. The building principal will designate an individual responsible for managing the school Web site. Teachers shall maintain their class site. Class sites may include individual student or group work. Parent permission must be obtained to publish student names or photos on the Web.

3. Extracurricular Organization Web Pages. With the approval of the building principal, extracurricular organizations may establish Web pages using district-provided web space. The principal or designee shall establish a process and posting of material on these pages. Material presented on the organization Web page must relate specifically to organization activities. Included materials must adhere to all other regulations and laws. Organization Web pages must include the following notice**:** "*This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the district."*

L. District Acceptable Use Policy

As stated in section G – Due Process of the SMYRNA SCHOOL DISTRICT Computing and Internet Board Policy (Policy 6150) existing policies govern student and employee behavior.

1. **Purpose:** In keeping with the Core Values and mission of the Smyrna School District the purpose of this policy is to establish acceptable and unacceptable use of the Covered Digital Resources provided by Smyrna School District, and the State of Delaware (collectively with Smyrna School District, the "District"), to Covered Users. Covered Digital Resources are provided for a education purpose for students and to facilitate employees' work productivity.

2. **Scope:** This policy applies to all users as covered in Section D of the SMYRNA SCHOOL DISTRICT Computing and Internet Board Policy (Policy 6150). **Digital Resources** are: (a) provided by the District; (b) paid for, in whole or in part, by the District; (c) used to conduct business or other activity for or on behalf of the District; or (d) used in or at a District facility. Covered Electronic Resources include, without limitation, the following:

a. **E-mail**, which includes to all electronic-mail accounts and services provided to Covered Users by the State of Delaware or SMYRNA SCHOOL DISTRICT;
b. **Computer Resources**, which includes all computers and related resources whether stationary or portable, including but not limited to all related peripherals, components, disk space, storage devices, cloud resources, servers, and output devices such as telephones, hand-held devices, printers, scanners, and copiers, whether owned or leased by the District;
c. **SMYRNA SCHOOL DISTRICT Network**, which includes the infrastructure used to transmit, store, and review data over an electronic medium, and includes any and all of the following technologies provided to authorized users: (a) Internet service; (b) intranet system; (c) SMYRNA SCHOOL DISTRICT mainframe system; and (d) any collaboration systems, including but not limited to calendaring, message boards, conference boards, blogs, text messaging, instant messaging, video conferencing, websites, and podcasting, whether the system is owned or contracted;
d. **Digital/Cloud Resource Data**, which includes any and all information, data, and material, accessed or posted through any Digital/Cloud Resource; all Smyrna School District staff are required to use exclusively the student database maintained by the State and currently available through Single SignOn access.
e. **Mobile Devices**, owned by the district or personally, which includes cellular phone, smartphone, tablets, or other electronic device connecting to the Network.

3. **General Guidelines for Use**
   a. Use of systems, static or mobile, network, data or media must reflect concern for children and their instruction. Professional conduct is expected at all times.
   b. Digital Resources are not intended for public access. The District has the right to place reasonable restrictions on the use of Digital Resources.
   c. Users are required to observe all rules and obligations set forth elsewhere by the District (for example, in the Employee Contracts or Student Code of Conduct) or by law at all times. This policy is intended to supplement, not replace, those expectations.
   d. Access to and use of Digital Resources is a privilege, not a right.
   e. Users will be responsible for any and all damage caused by their use of Digital Resources where such use does not comply with the requirements or purposes of this Policy. Responsibility may take the form of financial compensation, discipline, and/or restrictions on further use, as appropriate under the circumstances.

4. **Responsibilities**: Users have a responsibility to protect the security, integrity, and confidentiality of Digital Resources, including the obligation to protect and report any unauthorized access or use, abuse, misuse, degradation, theft, or destruction. Users shall comply with this Policy and all other applicable policies, rules, and laws, when using Digital Resources.

   a. District
      1. District officials are responsible for designating Users authorized to use Digital Resources.
      2. The District provides for the education of students regarding the Acceptable Use Policy and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and regarding cyber-bullying awareness and response.

b. **Students** have a responsibility to take reasonable steps to protect their privacy and personal information when using Digital Resources. Students must not disclose personal contact information, except to educational institutions for educational purposes, without prior approval. Students also must promptly disclose to a teacher or other appropriate District employee any violation of this Policy, including any message received that the student believes to be inappropriate or makes the student feel uncomfortable.

c. **District employees** that choose to communicate with students through email are expected to use District-provided e-mail and are strongly advised against using other forms of personal electronic communication with students, such as Instant Messaging or texting. In the event that there is a legitimate reason for an employee to communicate with students via electronic means other than District e-mail, the employee should use District endorsed methods/applications. District employees are required to take reasonable measures to protect their personal information and reputation when using Digital Resources or otherwise participating in activity online.

5. **Ownership**: All Digital Data created, transmitted, stored, and processed on the SMYRNA SCHOOL DISTRICT Network or Digital/Cloud Resources, are the property of the District. When a User is no longer affiliated with the District as an employee, contractor, or student, all information stored by that User on any Digital/Cloud Resource remains the property of the District.

6. **Unacceptable Uses:** Users are prohibited from using any Digital Resource to upload, post, mail, display, store, access, or transmit any inappropriate material or for any inappropriate purpose as set forth below. Cyber-bullying and other inappropriate online behavior off of the District network becomes the responsibility of the schools when the speech has caused or threatens to cause a substantial and material threat of disruption on campus or interference with the rights of students to be secure.

   a. Access to Inappropriate Material - It shall be a violation of this Policy for any User to use any Digital Resource to upload, post, mail, display, store, access, or transmit, any Inappropriate Material. Inappropriate Material is defined as any content, communication, or information that conflicts with the fundamental policies, Core Values and mission of the District. Whether material or content is considered inappropriate shall be determined without regard to whether such material or content has been blocked by any filtering software used by the District. Examples of Inappropriate Material include, but are not limited to, material that:

      1. is hateful, harassing, threatening, libelous, or defamatory;
      2. is deemed offensive or discriminatory based on race, religion, gender, age, national origin, citizenship, sexual orientation, mental or physical disability, marital status, or other characteristic protected by state, federal, or local law;
      3. constitutes use for, or in support of, any obscene or pornographic purpose including the transmission, review, retrieval, or access to any profane, obscene, or sexually explicit material;
      4. constitutes use for the solicitation or distribution of information intended or likely to incite violence or to harass, threaten, or stalk another individual;
      5. solicits or distributes information with the intent to cause personal harm or bodily injury;
      6. promotes or participates in any way in religious or political activities

b. Unlawful Purposes - It shall be a violation of this Policy for any User to use any Digital Resource for any purpose that:
   1. constitutes or furthers any unlawful activity;
   2. gives rise to civil liability under any applicable law, including U.S. patent, trademark, or copyright laws, including copyrighted software, music, videos, photos, clip art, or other images, including SMYRNA SCHOOL DISTRICT logos;
   3. impersonates any person, living or dead, organization, business, or other entity;
   4. enables or constitutes gaming, wagering, or gambling of any kind;
   5. promotes or participates in any way in unauthorized raffles or fundraisers;
   6. engages in private business, commercial, or other activities for personal financial gain.

c. Security Violations - It shall be a violation of this Policy for any User to use any Digital Resource in any way that threatens or violates the security of any Covered Technology, where such use:
   1. contains a virus, Trojan horse, logic bomb, malicious code, or other harmful component;
   2. constitutes a chain letter, junk mail, spam, or other similar electronic mail;
   3. constitutes unauthorized access or attempts to circumvent any security measures;
   4. obtains access to or use of another User's account, password, files, or data, or attempts to so access or use, without the express authorization of that other User;
   5. deprives a User of access to authorized access of Electronic Resources;
   6. engages in unauthorized or unlawful entry into a SMYRNA SCHOOL DISTRICT Network;
   7. shares e-mail addresses or distribution lists for uses that violate this Policy or any other District Policy;
   8. transmits sensitive or confidential information without appropriate security safeguards;
   9. falsifies, tampers with, or makes unauthorized changes or deletions to data located on the SMYRNA SCHOOL DISTRICT Network;
   10. obtains resources or SMYRNA SCHOOL DISTRICT Network access beyond those authorized;
   11. distributes unauthorized information regarding another User's password or security data;
   12. discloses confidential or proprietary information, including student record information, without authorization;
   13. involves the relocation of hardware (except for portable devices), installation of peripherals, or modification of settings to equipment without the express prior authorization by the District Technology Department.
   14. installs, downloads, or uses unauthorized or unlicensed software or third-party system without the express prior authorization by the District Technology Department;
   15. involves a deliberate attempt to disrupt the SMYRNA SCHOOL DISTRICT Network; and
   16. lead to costs to the SMYRNA SCHOOL DISTRICT (Excessive personal surfing, utilizing streaming services for personal use such as listening to music or watching video, and downloading of music and video files are specifically forbidden.)

7. Notice of Intent to Monitor: Users have no expectation of privacy in their use of and access to any Digital/Cloud Resource. District administrators and authorized personnel monitor the use of Digital/Cloud Resources to help ensure that uses are secure and in conformity with this Policy. The District reserves the right to examine, use, and disclose any data found on the SMYRNA SCHOOL DISTRICT Network or Digital/Cloud Resources in order to further the health, safety, discipline, or security of any student or other person, or to protect District property. It also may use this information in disciplinary actions and will furnish evidence of suspected criminal activity to law enforcement.

In recognition of the need to establish a safe and appropriate learning environment, the District will use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet.

8. **Limitation of Liability:** The District makes no warranties of any kind, neither express nor implied, for the Internet access it provides. The District will not be responsible for any damages any User suffers, including but not limited to, loss of data. The District will not be responsible for the accuracy, nature, or quality of information stored on the SMYRNA SCHOOL DISTRICT Network, nor for the accuracy, nature, or equality of information gathered through District-provided Internet access. The District will not be responsible for financial obligations arising through the unauthorized use of the network.

9. **Policy Violations:** The District will cooperate fully with local, state, and federal officials, in any investigation related to any alleged or suspected illegal activity conducted through the SMYRNA SCHOOL DISTRICT Network.
   a. The district cooperates with local, state, or federal officials in any investigation concerning or relating to any activities (requiring a mandatory report) conducted through the Network.
   b. Allegations a student violated the District Acceptable Use Policy are handled in accordance with the Student Code of Conduct.
   c. Allegations an employee violated the District Acceptable Use Policy are handled in accordance with the employee contract.
   d. The Superintendent or designee may terminate the account privileges of a guest user by providing notice to the user.

Attachments

Smyrna School District Student and Parent/Guardian Chromebook User Agreement

Revised and Approved by Board of Education, July 19, 2000
Revision Approved by Board of Education, May 20, 2012.
Revision Approved by Board of Education, November 19, 2014
Revision Approved by Board of Education, April 15, 2015
Revision Approved by Board of Education, March 15, 2017
Revision Approved by Board of Education, July 7, 2021